Bài 2.2: Mô phỏng PE loader 32bit & 64 bit

=====================================================

=====================================================

\*\*\*\*\*Load file PE 32bit của bài 1 check\_subdir.exe

OutPut 32bit:

Microsoft Windows [Version 10.0.26100.6584]

(c) Microsoft Corporation. All rights reserved.

L:\NCSS Malware Analyze\Bai 2.1 va 2.2>gcc -static -o pe\_loader.exe pe\_loader.c -lws2\_32 -ladvapi32 -luser32

L:\NCSS Malware Analyze\Bai 2.1 va 2.2>pe\_loader.exe

=== ADVANCED PE LOADER ===

Supports: Relocations, TLS Callbacks, Import Resolution

Please enter the path to the PE file (.exe):

> L:\NCSS Malware Analyze\Bai 2.1 va 2.2\check\_subdir.exe

[SUCCESS] File path validation passed: L:\NCSS Malware Analyze\Bai 2.1 va 2.2\check\_subdir.exe

[SUCCESS] File mapped at 0x010A0000, size: 0x0000DDBD bytes

[SUCCESS] PE file validation passed

=== FILE INFORMATION ===

File: L:\NCSS Malware Analyze\Bai 2.1 va 2.2\check\_subdir.exe

Architecture: 32-bit

Sections: 15

Image Base: 0x00400000

Entry Point: 0x0000102A

Image Size: 0x00012000 bytes

[INFO] Preferred base: 0x00400000, Image size: 0x00012000, Entry point: 0x0000102A

[SUCCESS] Image allocated at 0x00400000

[INFO] Image allocated at preferred base -> relocations NOT required

=== COPYING SECTIONS ===

[INFO] Copying 15 sections...

.text | VSz=0x00001C90 | VA=0x00001000 | RawSz=0x00001E00 | RawPtr=0x00000400 | Flags=0x60000020

.data | VSz=0x000000E0 | VA=0x00003000 | RawSz=0x00000200 | RawPtr=0x00002200 | Flags=0xC0000040

.rdata | VSz=0x00000CE0 | VA=0x00004000 | RawSz=0x00000E00 | RawPtr=0x00002400 | Flags=0x40000040

/4 | VSz=0x00000810 | VA=0x00005000 | RawSz=0x00000A00 | RawPtr=0x00003200 | Flags=0x40000040

.bss | VSz=0x000002AC | VA=0x00006000 | RawSz=0x00000000 | RawPtr=0x00000000 | Flags=0xC0000080

.idata | VSz=0x00000700 | VA=0x00007000 | RawSz=0x00000800 | RawPtr=0x00003C00 | Flags=0x40000040

.tls | VSz=0x00000008 | VA=0x00008000 | RawSz=0x00000200 | RawPtr=0x00004400 | Flags=0xC0000040

.reloc | VSz=0x000001E0 | VA=0x00009000 | RawSz=0x00000200 | RawPtr=0x00004600 | Flags=0x42000040

/14 | VSz=0x00000038 | VA=0x0000A000 | RawSz=0x00000200 | RawPtr=0x00004800 | Flags=0x42000040

/29 | VSz=0x00001172 | VA=0x0000B000 | RawSz=0x00001200 | RawPtr=0x00004A00 | Flags=0x42000040

/41 | VSz=0x000000B5 | VA=0x0000D000 | RawSz=0x00000200 | RawPtr=0x00005C00 | Flags=0x42000040

/55 | VSz=0x000000A0 | VA=0x0000E000 | RawSz=0x00000200 | RawPtr=0x00005E00 | Flags=0x42000040

/67 | VSz=0x00000038 | VA=0x0000F000 | RawSz=0x00000200 | RawPtr=0x00006000 | Flags=0x42000040

/80 | VSz=0x0000007A | VA=0x00010000 | RawSz=0x00000200 | RawPtr=0x00006200 | Flags=0x42000040

/91 | VSz=0x00000174 | VA=0x00011000 | RawSz=0x00000200 | RawPtr=0x00006400 | Flags=0x42000040

[INFO] Image loaded at preferred base 0x00400000, no relocation needed

[INFO] Processing imports...

Loading DLL: KERNEL32.dll

DeleteCriticalSection -> 0x77E14B20

EnterCriticalSection -> 0x77E04060

FreeLibrary -> 0x76BCD0E0

GetLastError -> 0x76BD33C0

GetModuleHandleA -> 0x76BCD5F0

GetProcAddress -> 0x76BC6780

InitializeCriticalSection -> 0x77E12890

LeaveCriticalSection -> 0x77E030E0

LoadLibraryA -> 0x76BE1C60

SetUnhandledExceptionFilter -> 0x76BCD2E0

Sleep -> 0x76BCD720

TlsGetValue -> 0x76BD33E0

VirtualProtect -> 0x76BC6B30

VirtualQuery -> 0x76BC8610

Loading DLL: api-ms-win-crt-environment-l1-1-0.dll

\_\_p\_\_environ -> 0x75C79160

Loading DLL: api-ms-win-crt-heap-l1-1-0.dll

\_set\_new\_mode -> 0x75C763D0

calloc -> 0x75C5B450

free -> 0x75C20080

malloc -> 0x75C20100

Loading DLL: api-ms-win-crt-locale-l1-1-0.dll

\_configthreadlocale -> 0x75C71920

Loading DLL: api-ms-win-crt-math-l1-1-0.dll

\_\_setusermatherr -> 0x75CBCDF0

Loading DLL: api-ms-win-crt-private-l1-1-0.dll

memcpy -> 0x75C87370

Loading DLL: api-ms-win-crt-runtime-l1-1-0.dll

\_\_p\_\_\_argc -> 0x75C77BF0

\_\_p\_\_\_argv -> 0x75C796D0

\_cexit -> 0x75CA1540

\_configure\_narrow\_argv -> 0x75C78EA0

\_crt\_atexit -> 0x75C51640

\_exit -> 0x75C75650

\_initialize\_narrow\_environment -> 0x75C77C00

\_initterm -> 0x75C55350

\_initterm\_e -> 0x75C55290

\_set\_app\_type -> 0x75C75A00

\_set\_invalid\_parameter\_handler -> 0x75C6BC20

abort -> 0x75C1DA20

exit -> 0x75C75670

signal -> 0x75C70730

Loading DLL: api-ms-win-crt-stdio-l1-1-0.dll

\_\_acrt\_iob\_func -> 0x75C6A170

\_\_p\_\_commode -> 0x75C779D0

\_\_p\_\_fmode -> 0x75C78180

\_\_stdio\_common\_vfprintf -> 0x75C176C0

gets -> 0x75CA22D0

Loading DLL: api-ms-win-crt-string-l1-1-0.dll

strlen -> 0x75C7D060

strncmp -> 0x75C7D240

[SUCCESS] Import resolution completed: 9 DLLs, 43 functions

[INFO] Executing TLS Callbacks...

Calling TLS Callback #1 at 0x00401880

[EXCEPTION] Code: 0xC0000005 at Address: 0x00401880

[WARNING] TLS Callback #1 caused exception

Calling TLS Callback #1 at 0x00401910

[EXCEPTION] Code: 0xC0000005 at Address: 0x00401910

[WARNING] TLS Callback #1 caused exception

[SUCCESS] Executed 0 TLS Callbacks

[INFO] Setting section permissions...

.text : 0x00401000 -> RX

.data : 0x00403000 -> RW

.rdata : 0x00404000 -> RO

/4 : 0x00405000 -> RO

.bss : 0x00406000 -> RW

.idata : 0x00407000 -> RO

.tls : 0x00408000 -> RW

.reloc : 0x00409000 -> RO

/14 : 0x0040A000 -> RO

/29 : 0x0040B000 -> RO

/41 : 0x0040D000 -> RO

/55 : 0x0040E000 -> RO

/67 : 0x0040F000 -> RO

/80 : 0x00410000 -> RO

/91 : 0x00411000 -> RO

=== READY TO EXECUTE ===

Entry Point: 0x0040102A

Press:

1 - Execute program

2 - Exit without execution

Trường hợp nhập 1 sẽ chạy file PE:

[EXECUTING] Transferring control to entry point...

\*\*\*\*\*Enter base directory\*\*\*\*\*: C:\

\*\*\*\*\*Enter subdirectory to check\*\*\*\*\*: C:\123

TRUE

Trường hợp nhập 2:

[INFO] Execution cancelled by user

[CLEANUP] Releasing allocated resources...

Freed image memory at 0x00DF0000

Unmapped file view

Closed file mapping

Closed file handle

[SUCCESS] Cleanup completed

Press Enter to exit...

L:\NCSS Malware Analyze\Bai 2.1 va 2.2>

=====================================================

=====================================================

=====================================================

=====================================================

\*\*\*\*\*Load file 64bit (check\_range64bit.exe tự build)

Output 64bit:

L:\NCSS Malware Analyze\Bai 2.1 va 2.2>pe\_loader64.exe

=== 64-BIT ADVANCED PE LOADER ===

Please enter the path to the 64-bit PE file (.exe):

> check\_range64bit.exe

[SUCCESS] File path validation passed: check\_range64bit.exe

[SUCCESS] File mapped at 0x0000013C95020000, size: 0x0002234E bytes

[SUCCESS] 64-bit PE file validation passed

=== 64-BIT FILE INFORMATION ===

File: check\_range64bit.exe

Architecture: 64-bit (AMD64)

Sections: 19

Image Base: 0x0000000140000000

Entry Point: 0x00001400

Image Size: 0x00025000 bytes

Subsystem: 3

Characteristics: 0x0026

[INFO] Preferred base: 0x0000000140000000, Image size: 0x00025000

[SUCCESS] 64-bit Image allocated at 0x0000000140000000

=== COPYING 64-BIT SECTIONS ===

[INFO] Copying 19 sections...

.text | VSz=0x00001940 | VA=0x00001000 | RawSz=0x00001A00 | RawPtr=0x00000600 | Flags=0x60000020

.data | VSz=0x000000B0 | VA=0x00003000 | RawSz=0x00000200 | RawPtr=0x00002000 | Flags=0xC0000040

.rdata | VSz=0x00000C68 | VA=0x00004000 | RawSz=0x00000E00 | RawPtr=0x00002200 | Flags=0x40000040

.pdata | VSz=0x00000228 | VA=0x00005000 | RawSz=0x00000400 | RawPtr=0x00003000 | Flags=0x40000040

.xdata | VSz=0x000001B4 | VA=0x00006000 | RawSz=0x00000200 | RawPtr=0x00003400 | Flags=0x40000040

.bss | VSz=0x00000180 | VA=0x00007000 | RawSz=0x00000000 | RawPtr=0x00000000 | Flags=0xC0000080

.idata | VSz=0x00000864 | VA=0x00008000 | RawSz=0x00000A00 | RawPtr=0x00003600 | Flags=0x40000040

.tls | VSz=0x00000010 | VA=0x00009000 | RawSz=0x00000200 | RawPtr=0x00004000 | Flags=0xC0000040

.rsrc | VSz=0x000004E8 | VA=0x0000A000 | RawSz=0x00000600 | RawPtr=0x00004200 | Flags=0x40000040

.reloc | VSz=0x00000060 | VA=0x0000B000 | RawSz=0x00000200 | RawPtr=0x00004800 | Flags=0x42000040

/4 | VSz=0x00000540 | VA=0x0000C000 | RawSz=0x00000600 | RawPtr=0x00004A00 | Flags=0x42000040

/19 | VSz=0x0000B3BA | VA=0x0000D000 | RawSz=0x0000B400 | RawPtr=0x00005000 | Flags=0x42000040

/31 | VSz=0x000022FF | VA=0x00019000 | RawSz=0x00002400 | RawPtr=0x00010400 | Flags=0x42000040

/45 | VSz=0x00001F2B | VA=0x0001C000 | RawSz=0x00002000 | RawPtr=0x00012800 | Flags=0x42000040

/57 | VSz=0x000008D8 | VA=0x0001E000 | RawSz=0x00000A00 | RawPtr=0x00014800 | Flags=0x42000040

/70 | VSz=0x000002D2 | VA=0x0001F000 | RawSz=0x00000400 | RawPtr=0x00015200 | Flags=0x42000040

/81 | VSz=0x00001C37 | VA=0x00020000 | RawSz=0x00001E00 | RawPtr=0x00015600 | Flags=0x42000040

/97 | VSz=0x000012A6 | VA=0x00022000 | RawSz=0x00001400 | RawPtr=0x00017400 | Flags=0x42000040

/113 | VSz=0x0000018C | VA=0x00024000 | RawSz=0x00000200 | RawPtr=0x00018800 | Flags=0x42000040

[INFO] Image loaded at preferred base 0x0000000140000000, no relocation needed

[INFO] Processing 64-bit imports...

Loading DLL: KERNEL32.dll

DeleteCriticalSection -> 0x00007FF9B66B9240

EnterCriticalSection -> 0x00007FF9B667BF00

GetLastError -> 0x00007FF9B5AC8640

InitializeCriticalSection -> 0x00007FF9B6604670

LeaveCriticalSection -> 0x00007FF9B667C000

SetUnhandledExceptionFilter -> 0x00007FF9B5AF3600

Sleep -> 0x00007FF9B5AE1980

TlsGetValue -> 0x00007FF9B5B34490

VirtualProtect -> 0x00007FF9B5AE82B0

VirtualQuery -> 0x00007FF9B5AE82F0

Loading DLL: api-ms-win-crt-environment-l1-1-0.dll

\_\_p\_\_environ -> 0x00007FF9B4032910

Loading DLL: api-ms-win-crt-heap-l1-1-0.dll

\_set\_new\_mode -> 0x00007FF9B3FDD2B0

calloc -> 0x00007FF9B3FA6F50

free -> 0x00007FF9B3FB5DE0

malloc -> 0x00007FF9B3FB5E00

Loading DLL: api-ms-win-crt-locale-l1-1-0.dll

\_configthreadlocale -> 0x00007FF9B4024020

Loading DLL: api-ms-win-crt-math-l1-1-0.dll

\_\_setusermatherr -> 0x00007FF9B406FBE0

Loading DLL: api-ms-win-crt-private-l1-1-0.dll

\_\_C\_specific\_handler -> 0x00007FF9B40514D0

memcpy -> 0x00007FF9B408DB00

Loading DLL: api-ms-win-crt-runtime-l1-1-0.dll

\_\_p\_\_\_argc -> 0x00007FF9B4031270

\_\_p\_\_\_argv -> 0x00007FF9B4036AF0

\_cexit -> 0x00007FF9B403DD90

\_configure\_narrow\_argv -> 0x00007FF9B4037120

\_crt\_atexit -> 0x00007FF9B40186D0

\_exit -> 0x00007FF9B4044AF0

\_initialize\_narrow\_environment -> 0x00007FF9B4031260

\_set\_app\_type -> 0x00007FF9B4024B70

\_initterm -> 0x00007FF9B400E6E0

\_initterm\_e -> 0x00007FF9B4013220

\_set\_invalid\_parameter\_handler -> 0x00007FF9B401EFA0

abort -> 0x00007FF9B4044A80

exit -> 0x00007FF9B4030CA0

signal -> 0x00007FF9B40230C0

Loading DLL: api-ms-win-crt-stdio-l1-1-0.dll

\_\_acrt\_iob\_func -> 0x00007FF9B40122A0

\_\_p\_\_commode -> 0x00007FF9B4029160

\_\_p\_\_fmode -> 0x00007FF9B4038C10

\_\_stdio\_common\_vfprintf -> 0x00007FF9B3FD4620

\_\_stdio\_common\_vfscanf -> 0x00007FF9B4030CB0

puts -> 0x00007FF9B3FD5CB0

Loading DLL: api-ms-win-crt-string-l1-1-0.dll

strlen -> 0x00007FF9B408D120

strncmp -> 0x00007FF9B408D390

[SUCCESS] 64-bit import resolution completed: 9 DLLs, 41 functions

[INFO] Executing 64-bit TLS Callbacks...

Calling 64-bit TLS Callback #1 at 0x0000000140001570

[EXCEPTION] Code: 0xC0000005 at Address: 0x0000000140001570

[WARNING] 64-bit TLS Callback #1 caused exception

Calling 64-bit TLS Callback #1 at 0x0000000140001550

[EXCEPTION] Code: 0xC0000005 at Address: 0x0000000140001550

[WARNING] 64-bit TLS Callback #1 caused exception

[SUCCESS] Executed 0 64-bit TLS Callbacks

[INFO] Setting 64-bit section permissions...

.text : 0x0000000140001000 -> RX

.data : 0x0000000140003000 -> RW

.rdata : 0x0000000140004000 -> RO

.pdata : 0x0000000140005000 -> RO

.xdata : 0x0000000140006000 -> RO

.bss : 0x0000000140007000 -> RW

.idata : 0x0000000140008000 -> RO

.tls : 0x0000000140009000 -> RW

.rsrc : 0x000000014000A000 -> RO

.reloc : 0x000000014000B000 -> RO

/4 : 0x000000014000C000 -> RO

/19 : 0x000000014000D000 -> RO

/31 : 0x0000000140019000 -> RO

/45 : 0x000000014001C000 -> RO

/57 : 0x000000014001E000 -> RO

/70 : 0x000000014001F000 -> RO

/81 : 0x0000000140020000 -> RO

/97 : 0x0000000140022000 -> RO

/113 : 0x0000000140024000 -> RO

=== 64-BIT EXECUTION READY ===

Entry Point: 0x0000000140001400

Press:

1 - Execute 64-bit program

2 - Exit without execution

- Trường hợp nhập 1:

[EXECUTING] Transferring control to 64-bit entry point...

Enter (0 to quit): 3

true

Enter (0 to quit): 11

false

Enter (0 to quit): 0

- Trường hợp nhập 2:

[INFO] 64-bit execution cancelled by user

[CLEANUP] Releasing allocated resources...

Freed image memory at 0x0000000140000000

Unmapped file view

Closed file mapping

Closed file handle

[SUCCESS] Cleanup completed

Press Enter to exit...

L:\NCSS Malware Analyze\Bai 2.1 va 2.2>

=====================================================

=====================================================

=====================================================

\*\*\*Điều kiện bài 2.2 mà CODE đã hoàn thành:

**✅ Các yêu cầu đã hoàn thành đầy đủ:**

**1. Đọc file PE từ đĩa**

* Code sử dụng CreateFileA, CreateFileMappingA, và MapViewOfFile để map file vào memory một cách hiệu quả.
* Output xác nhận: [SUCCESS] File mapped at 0x015A0000, size: 0x0000DDBD bytes.

**2. Cấp phát bộ nhớ theo ImageBase/SizeOfImage**

* Code sử dụng VirtualAlloc để cấp phát bộ nhớ với kích thước SizeOfImage và ưu tiên tại ImageBase mong muốn (0x00400000). Nếu không được, nó sẽ cấp phát tại địa chỉ khác.
* Output xác nhận: [SUCCESS] Image allocated at 0x00400000.

**3. Ánh xạ các section đúng địa chỉ RVA**

* Code copy các section từ file vào bộ nhớ dựa trên VirtualAddress và SizeOfRawData, đồng thời xử lý zero-fill cho các section như .bss.
* Output hiển thị chi tiết từng section: [INFO] Copying 15 sections... với địa chỉ VA và kích thước.

**4. Xử lý Entry Point**

* Sau khi load xong, code cho phép người dùng chọn thực thi entry point. Khi chọn, nó gọi hàm tại ImageBase + AddressOfEntryPoint (0x0040102A).
* Output xác nhận: [EXECUTING] Transferring control to entry point... và chương trình gốc chạy thành công (nhập liệu và trả về "TRUE").

**5. Xử lý lỗi và validate PE**

* Hàm ValidatePE kiểm tra:
  + DOS signature ("MZ") và PE signature ("PE").
  + Chỉ hỗ trợ file 32-bit (Machine = 0x014C).
  + Số section hợp lý (tránh file độc hại).
  + Entry Point không vượt quá kích thước image.
* Code sử dụng cơ chế bắt exception thông qua setjmp/longjmp và AddVectoredExceptionHandler để xử lý lỗi trong quá trình load (ví dụ: TLS callbacks gây exception).

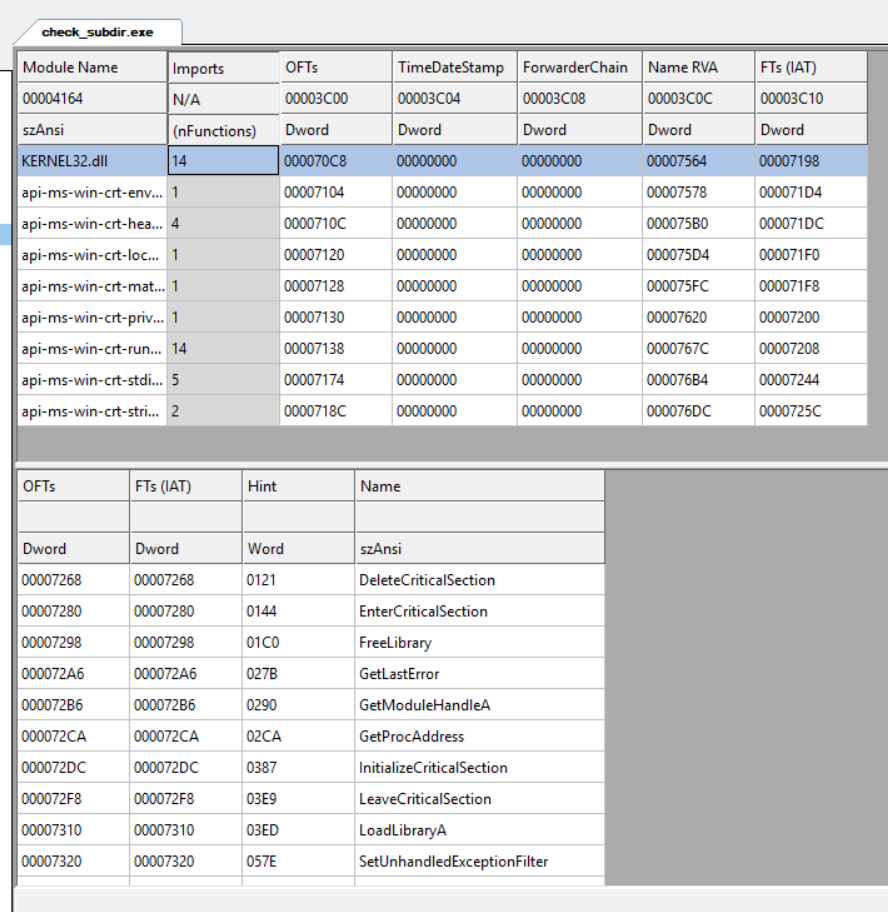
**✅ Các tính năng khác:**

**1. Xử lý Relocation**

* Code kiểm tra và áp dụng relocation nếu image được load tại địa chỉ khác với ImageBase mong muốn. Trong trường hợp này, không cần vì load đúng base.

**2. Resolve Import Table**

* Load các DLL cần thiết và lấy địa chỉ hàm thông qua LoadLibraryA và GetProcAddress.
* Output hiển thị chi tiết: [SUCCESS] Import resolution completed: 9 DLLs, 43 functions.



**3. Thực thi TLS Callbacks**

* Code thực thi các TLS callback trước khi vào entry point (dù có exception trong callback, nhưng đã xử lý an toàn).
* Output: [INFO] Executing TLS Callbacks... và bắt được exception.

**4. Thiết lập quyền truy cập bộ nhớ (Section Permissions)**

* Đặt permissions (RX, RW, RO) cho từng section dựa trên characteristics.
* Output: [INFO] Setting section permissions... với các quyền tương ứng.

**5. Cleanup tài nguyên**

* Hàm CleanupResources giải phóng bộ nhớ, unmapped file, và đóng handle đúng cách.

END!