

## 一、 修改 PE 文件导入表 (notepad\_patch.exe)

### 1. 首先使用 PEView 打开原 notepad.exe 查看 IMPORT Directory Table 字段

pFile	Data	Description	Value
00000400	77C71436	Virtual Address	027F RegSetValueExW
00000404	77C74615	Virtual Address	026F RegQueryValueExW
00000408	77C74605	Virtual Address	0231 RegCloseKey
0000040C	77C71474	Virtual Address	023D RegCreateKeyW
00000410	77C745F5	Virtual Address	0262 RegOpenKeyExW
00000414	77C743F6	Virtual Address	0181 IsTextUnicode
00000418	77C735FC	Virtual Address	0057 CloseServiceHandle
0000041C	77C6B4D7	Virtual Address	0225 QueryServiceConfigW
00000420	77C6C9EC	Virtual Address	01FC OpenServiceW
00000424	77C6CA04	Virtual Address	01FA OpenSCManagerW
00000428	00000000	End of Imports	ADVAPI32.dll
0000042C	77E2BF25	Virtual Address	01EB GetFileInformationByHandle
00000430	77E45716	Virtual Address	0141 FindNLSString
00000434	77E2A29D	Virtual Address	02B4 GlobalAlloc
00000438	77E2A2FB	Virtual Address	02C6 GlobalUnlock
0000043C	77E2A3AD	Virtual Address	02BF GlobalLock
00000440	77E2B138	Virtual Address	0297 GetTimeFormatW
00000444	77E2B31A	Virtual Address	01C9 GetDateFormatW
00000448	77E2AC67	Virtual Address	0202 GetLocalTime
0000044C	77E22CF3	Virtual Address	029E GetUserDefaultUILanguage
00000450	77E2C4D0	Virtual Address	02D0 HeapFree
00000454	77F12DA6	Virtual Address	02CC HeapAlloc
00000458	77E2F7C4	Virtual Address	02D4 HeapSetInformation
0000045C	77E21384	Virtual Address	008D CreateFileMappingW
00000460	77E2C562	Virtual Address	02ED InterlockedExchange
00000464	77E204E0	Virtual Address	0164 FreeLibraryAndExitThread
00000468	77E34D2C	Virtual Address	01E9 GetFileAttributesW
0000046C	77E702C9	Virtual Address	051C Wow64RevertWow64FsRedirection
00000470	77E1C364	Virtual Address	0518 Wow64DisableWow64FsRedirection
00000474	77E255A6	Virtual Address	030F IsWow64Process
00000478	77E2D8B0	Virtual Address	01C1 GetCurrentProcess
0000047C	77E2DDD2	Virtual Address	00B6 CreateThread
00000480	77E2F052	Virtual Address	0340 LoadLibraryW
00000484	77E2F045	Virtual Address	0213 GetModuleFileNameW
00000488	77E28F48	Virtual Address	015F FormatMessageW
0000048C	77E29553	Virtual Address	0357 MapViewOfFile
00000490	77E2F017	Virtual Address	0367 MultiByteToWideChar
00000494	77E2F84C	Virtual Address	04DB UnmapViewOfFile
00000498	77E2F84C	Virtual Address	04DB UnmapViewOfFile

### 2. 确定原 IMPORT Directory Table 的 RAW 和 RVA 分别为 0x94dc 和 0xa0a0, 计划将其移动至 SECTION .reloc 节的末尾空间, 得到如下移动方案: 0x94a0-0x95b8 复制到 0x2bc50-0x2bd68

#### a) 移动前位置

000094A0	8C A2 00 00 FF FF FF FF	FF FF FF FF 7C A2 00 00	Gc` yyyyyyyyy c`
000094B0	00 10 00 00 B8 A2 00 00	FF FF FF FF FF FF FF FF	.c` yyyyyyyyy
000094C0	6C A2 00 00 2C 10 00 00	DC A3 00 00 FF FF FF FF	lc` , Üe` yyyý
000094D0	FF FF FF FF 60 A2 00 00	50 11 00 00 38 A4 00 00	yyyy`c` P` 8m`
000094E0	FF FF FF FF FF FF FF FF	54 A2 00 00 AC 11 00 00	yyyyyyyyTc` -`
000094F0	68 A5 00 00 FF FF FF FF	FF FF FF FF 48 A2 00 00	h#` yyyyyyyyyHc`
00009500	DC 12 00 00 C8 A5 00 00	FF FF FF FF FF FF FF FF	Ü` È#` yyyyyyyyy
00009510	38 A2 00 00 3C 13 00 00	F0 A5 00 00 FF FF FF FF	8c` <` 8#` yyyý
00009520	FF FF FF FF 2C A2 00 00	64 13 00 00 14 A6 00 00	yyyy,c` d` !`
00009530	FF FF FF FF FF FF FF FF	1C A2 00 00 88 13 00 00	yyyyyyyy`c` ^`
00009540	24 A6 00 00 FF FF FF FF	FF FF FF FF 10 A2 00 00	\$!` yyyyyyyyy`c`
00009550	98 13 00 00 40 A6 00 00	FF FF FF FF FF FF FF FF	~` @!` yyyyyyyyy
00009560	04 A2 00 00 B4 13 00 00	4C A6 00 00 FF FF FF FF	`c` ^` L!` yyyý
00009570	FF FF FF FF F4 A1 00 00	C0 13 00 00 60 A6 00 00	yyyyó;` À` !`
00009580	FF FF FF FF FF FF FF FF	E4 A1 00 00 D4 13 00 00	yyyyyyyya;` Ó`
00009590	6C A6 00 00 FF FF FF FF	FF FF FF FF D8 A1 00 00	l!` yyyyyyyyyó;
000095A0	E0 13 00 00 80 A6 00 00	FF FF FF FF FF FF FF FF	à` €!` yyyyyyyyy

## b) 移动后位置

0002BC50	8C A2 00 00 FF FF FF FF	FF FF FF FF 7C A2 00 00	Gc` yyyyyyyyy c`
0002BC60	00 10 00 00 B8 A2 00 00	FF FF FF FF FF FF FF FF	.c` yyyyyyyyy
0002BC70	6C A2 00 00 2C 10 00 00	DC A3 00 00 FF FF FF FF	lc` , Üe` yyyý
0002BC80	FF FF FF FF 60 A2 00 00	50 11 00 00 38 A4 00 00	yyyy`c` P` 8m`
0002BC90	FF FF FF FF FF FF FF FF	54 A2 00 00 AC 11 00 00	yyyyyyyyTc` -`
0002BCA0	68 A5 00 00 FF FF FF FF	FF FF FF FF 48 A2 00 00	h#` yyyyyyyyyHc`
0002BCB0	DC 12 00 00 C8 A5 00 00	FF FF FF FF FF FF FF FF	Ü` È#` yyyyyyyyy
0002BCC0	38 A2 00 00 3C 13 00 00	F0 A5 00 00 FF FF FF FF	8c` <` 8#` yyyý
0002BCD0	FF FF FF FF 2C A2 00 00	64 13 00 00 14 A6 00 00	yyyy,c` d` !`
0002BCE0	FF FF FF FF FF FF FF FF	1C A2 00 00 88 13 00 00	yyyyyyyy`c` ^`
0002BCF0	24 A6 00 00 FF FF FF FF	FF FF FF FF 10 A2 00 00	\$!` yyyyyyyyy`c`
0002BD00	98 13 00 00 40 A6 00 00	FF FF FF FF FF FF FF FF	~` @!` yyyyyyyyy
0002BD10	04 A2 00 00 B4 13 00 00	4C A6 00 00 FF FF FF FF	`c` ^` L!` yyyý
0002BD20	FF FF FF FF F4 A1 00 00	C0 13 00 00 60 A6 00 00	yyyyó;` À` !`
0002BD30	FF FF FF FF FF FF FF FF	E4 A1 00 00 D4 13 00 00	yyyyyyyya;` Ó`
0002BD40	6C A6 00 00 FF FF FF FF	FF FF FF FF D8 A1 00 00	l!` yyyyyyyyyó;
0002BD50	E0 13 00 00 80 A6 00 00	FF FF FF FF FF FF FF FF	à` €!` yyyyyyyyy

- 在尾部增加 MyD113.dll 的 IMAGE\_IMPORT\_DESCRIPTOR，主要是 5 个字段；与课件中的方式不同，我将增加的 INT 和 IAT 表以及 DLL 名字和导入函数名字的字符串都放在了 SECTION .reloc 的末尾空间：

### a) 确定 Name RVA

“MyD113.dll” 字符串被放在了 RAW 0x2bd90，计算得 RVA: **0x2bd90-0x2ae00+0x2f000=0x2ffb0**

### b) TimeDateStamp 和 ForwarderChain 设为 0xffffffff

- 把 INT 布置到 RAW 0x2bdb0，将 “\x00\x00dummy” 保存到 RAW 0x2bda0，由于 INT 得第一项便是 dummy，所以 0x2bdb0 上保存的指针为 RAW 0x2bda0；计算出 INT 的 RVA 为 **0x2ffb0**

### d) 将 IAT 布置在 RAW 0x2bdc0，计算得 IAT 的 RVA 为 **0x2ffc0**

最后得到的结果如下：

0002BC50	8C A2 00 00 FF FF FF FF	FF FF FF FF 7C A2 00 00	Ge yyyyyyyyy c
0002BC60	00 10 00 00 B8 A2 00 00	FF FF FF FF FF FF FF FF	.c yyyyyyyyy
0002BC70	6C A2 00 00 2C 10 00 00	DC A3 00 00 FF FF FF FF	1c , Üe yyy
0002BC80	FF FF FF FF 60 A2 00 00	50 11 00 00 38 A4 00 00	yyyy`c P 8x
0002BC90	FF FF FF FF FF FF FF FF	54 A2 00 00 AC 11 00 00	yyyyyyTc -
0002BCA0	68 A5 00 00 FF FF FF FF	FF FF FF FF 48 A2 00 00	h¥ yyyyyyyHc
0002BCB0	DC 12 00 00 C8 A5 00 00	FF FF FF FF FF FF FF FF	Ü E¥ yyyyyyy
0002BCC0	38 A2 00 00 3C 13 00 00	F0 A5 00 00 FF FF FF FF	8c < 8¥ yyy
0002BCD0	FF FF FF FF 2C A2 00 00	64 13 00 00 14 A6 00 00	yyyy,c d !
0002BCE0	FF FF FF FF FF FF FF FF	1C A2 00 00 88 13 00 00	yyyyyy c ^
0002BCF0	24 A6 00 00 FF FF FF FF	FF FF FF FF 10 A2 00 00	\$! yyyyyyy c
0002BD00	98 13 00 00 40 A6 00 00	FF FF FF FF FF FF FF FF	~ @! yyyyyyy
0002BD10	04 A2 00 00 B4 13 00 00	4C A6 00 00 FF FF FF FF	c ' L! yyy
0002BD20	FF FF FF FF F4 A1 00 00	C0 13 00 00 60 A6 00 00	yyyyö; Å `!
0002BD30	FF FF FF FF FF FF FF FF	E4 A1 00 00 D4 13 00 00	yyyyyya; ö
0002BD40	6C A6 00 00 FF FF FF FF	FF FF FF FF D8 A1 00 00	1! yyyyyyyö;
0002BD50	E0 13 00 00 80 A6 00 00	FF FF FF FF FF FF FF FF	à €! yyyyyyy
0002BD60	CC A1 00 00 F4 13 00 00	B0 FF 02 00 FF FF FF FF	î; ö °y yyy
0002BD70	FF FF FF FF 90 FF 02 00	C0 FF 02 00 00 00 00 00	yyyy y Ày
0002BD80	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0002BD90	4D 79 44 6C 6C 33 2E 64	6C 6C 00 00 00 00 00 00	MyDll3.dll
0002BDA0	00 00 64 75 6D 6D 79 00	00 00 00 00 00 00 00 00	dummy
0002BDB0	A0 FF 02 00 00 00 00 00	00 00 00 00 00 00 00 00	y
0002BDC0	FF FF FF FF 00 00 00 00	00 00 00 00 00 00 00 00	yyyy
0002BDD0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0002BDE0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0002BDF0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

4. 由于 IAT 表在运行时会被覆盖为函数地址，所以需要给予 SECTION .reloc 可写权限，即在 SECTION .reloc 原来属性值的基础上加上 0x80000000 得到 0xc200040，而 SECTION .reloc 属性值存在 RAW 0x26c，于是到对应位置做修改：

a) 修改前属性值

pFile	Data	Description	Value
00000248	2E 72 65 6C	Name	.reloc
0000024C	6F 63 00 00		
00000250	00000E38	Virtual Size	
00000254	0002F000	RVA	
00000258	00001000	Size of Raw Data	
0000025C	0002AE00	Pointer to Raw Data	
00000260	00000000	Pointer to Relocations	
00000264	00000000	Pointer to Line Numbers	
00000268	0000	Number of Relocations	
0000026A	0000	Number of Line Numbers	
0000026C	42000040	Characteristics	
	00000040	IMAGE_SCN_CNT_INITIALIZED_DATA	
	02000000	IMAGE_SCN_MEM_DISCARDABLE	
	40000000	IMAGE_SCN_MEM_READ	

b) 修改位置

00000240	00 00 00 00 40 00 00 40	2E 72 65 6C 6F 63 00 00	ü
00000250	38 0E 00 00 00 F0 02 00	00 10 00 00 00 AE 02 00	8 ü
00000260	00 00 00 00 00 00 00 00	00 00 00 00 40 00 00 C2	
00000270	C2 B0 9E 55 80 00 00 00	E0 B1 9E 55 8D 00 01 00	Ä°žü€
00000280	0E B2 8F 55 8A 00 00 00	FB B3 8F 55 8A 00 00 00	£žü£

c) 修改后属性值

pFile	Data	Description	Value
00000248	2E 72 65 6C	Name	.reloc
0000024C	6F 63 00 00		
00000250	00000E38	Virtual Size	
00000254	0002F000	RVA	
00000258	00001000	Size of Raw Data	
0000025C	0002AE00	Pointer to Raw Data	
00000260	00000000	Pointer to Relocations	
00000264	00000000	Pointer to Line Numbers	
00000268	0000	Number of Relocations	
0000026A	0000	Number of Line Numbers	
0000026C	C2000040	Characteristics	
	00000040	IMAGE_SCN_CNT_INITIALIZED_DATA	
	02000000	IMAGE_SCN_MEM_DISCARDABLE	
	40000000	IMAGE_SCN_MEM_READ	
	80000000	IMAGE_SCN_MEM_WRITE	

5. 删除（置0）IMAGE\_OPTION\_HEADER 中的 BOUND\_IMPORT Table 字段，以保证添加的 DLL 可以正常加载

a) 修改前

000001A4	00000040	Size	
000001A8	00000270	RVA	BOUND_IMPORT Table
000001AC	00000128	Size	

b) 修改后

000001A8	00000000	RVA	BOUND_IMPORT Table
000001AC	00000128	Size	

6. 尝试运行并使用 Process Explorer 观察 DLL 加载结果，观察文件下载是否成功

a) DLL 加载成功

notepad_patch.exe	9,352 K	24,088 K < 0.01	398
processp_Chn.exe	7,616 K	11,504 K	472
processp_Chn64.exe	54,820 K	75,220 K < 47.16	279
SGTool.exe	16,368 K	27,228 K < 0.01	280
GoogleCrashHandler.exe	1,484 K	1,540 K	287
GoogleCrashHandler64.exe	1,532 K	1,380 K	288
IEMonitor.exe	9,448 K	19,188 K < 0.01	218
SogouCloud.exe	11,592 K	21,880 K	372

  

名称	描述	公司名称
locale.nls		
lpk.dll	Language Pack	Microsoft Corporati
msasn1.dll	ASN.1 Runtime APIs	Microsoft Corporati
msctf.dll	MSCTF 服务器 DLL	Microsoft Corporati
msimg32.dll	GDIEXT Client DLL	Microsoft Corporati
msvcr100.dll	Microsoft® C Runtime Library	Microsoft Corporati
msvcr71.dll	Windows NT CRT DLL	Microsoft Corporati
mswsock.dll	Microsoft Windows Sockets ...	Microsoft Corporati
MyDll3.dll		
NapiNSP.dll	电子邮件命名填充提供程序	Microsoft Corporati
ntevent.dll	Windows 加电库	Microsoft Corporati

b) DLL 功能正常，成功下载网页

index.html	2021/11/2 16:48	Chrome HTML D...	524 KB
MyDll3.dll	2021/11/1 23:31	应用程序扩展	7 KB