目录

回顾	1
Winasm_0.exe 分析	
常用程序的特征	
分析 BC++程序特征	
分析 Delphi 程序特征	
分析 VS 程序	5
分析 vc6.0 和易语言	

回顾

1. IDA 的快捷键有哪些?

空格 切换选项卡

R 转换为 ASCii 码字符

N 重命名

G 打开跳转窗口

INS 打开创建结构体窗口(结构体窗口)

Q 将局部变量转为本身数值

Shift+F4 打开名称窗口

M 转换常量数据为宏定义

回车 选中地址按回车进入到地址内部

D 定义数据类型

Alt+Q 转换结构体类型(局部堆栈窗口)

F5 将反汇编反编译为 C 代码

Alt+M 添加标签

 A
 转换为 Ascii 码字符串

 Tab
 将反汇编反编译为 C 代码

ESC 返回上一步 : 添加注释

Alt+G 切换指令集(ARM 指令与 thumb 指令转换)

C 将数据转为代码 Ctrl+P 打开函数窗口 Alt+T 搜索文本 Ctrl+X 交叉引用

F7 单步步入(调试器) F8 单步步过(调试器)

? 打开计算器Ctrl+M 打开标签窗口Ctrl+Alt+B 断点列表F1 查看帮助文档

Ctrl+F7 运行到函数返回地址

```
Shift+F9 打开结构体窗口
```

U 将当前选中的数据会代码转为未定义

Ctrl+K打开局部堆栈窗口Shift+F3打开函数窗口Shift+F12字符串窗口

Alt+K 打开设置堆栈窗口 P 将代码转为函数

Winasm_0.exe 分析

```
0334A
0334A pExceptionInfo = dword ptr 8
0334A
0334A
                                                                    ; push ebp
                                enter
                                            ; mov ebp, esp
esi ; 保存寄存器环境
esi, [ebp+pExceptionInfo]
0334A
0334E
                                push
0334F
                                 mov
                                                                    ; eax = [esi] = pExceptionRecord
; esi += 4
03352
                                lodsd
03352
                                                                    ; eax = [eax] = [pExceptionRecord] = ExceptionCode
; = 0xC0000005
03353
                                mov
                                            eax, [eax]
03353
                                            ; = 0xC0000005
eax, 0DEADFFh ; eax = 0xC0000005 & 0xDEADFF = 5
eax, 5 ; eax << 5 = 0xA0
ebx, eax ; ebx = eax = 0xA0 |
eax, [eax+402FAEh] ; eax = 0xA0 + 0x402FAE = 0x40304E
esi, [esi] ; esi = [esi] = pContextRecord
[esi+CONTEXT._Edi], eax ; 修改 Context.edi = 40304E
03355
                                 and
0335A
                                 sh1
0335D
                                mov
0335F
                                1ea
03365
                                mov
03367
                                mov
0336D
                                 add
                                            eax, 2DCh
03372
                                 mov
                                            [ebx+esi], eax ; 修改 Context.ESI = 40332A
03375
                                mov
                                            eax, 400FDFh
0337A
                                 add
                                            eax, ebx
                                            [esi+CONTEXT._Eip], eax ; 修改 Context.eip = 40107F
0337C
                                mov
03382
                                 xor
                                            eax, eax
                                                                    ; 返回值是-1 继续回到修改后EIP处执行
; 恢复寄存器环境
; mov esp,ebp
03384
                                dec
                                            eax
03385
                                pop
leave
                                            esi
03386
03386
                                                                    ; pop ebp
```

常用程序的特征

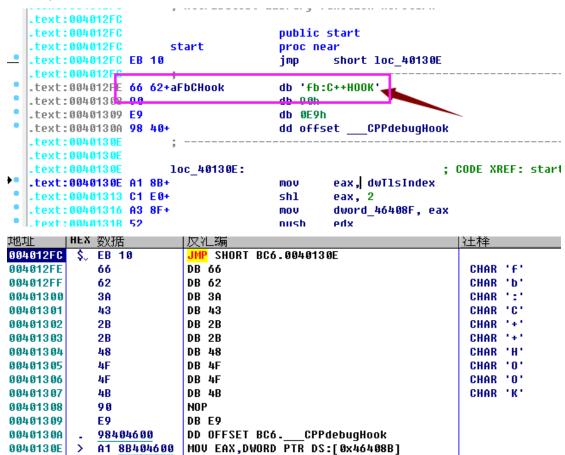
- 1. BC++
- 2. Delphi
- 3. 易语言
- 4. VB
- 5. VC++

分析 BC++程序特征

1. OEP 特征

- 2. 区段名称
- 3. 链接器版本

1. Oep 特征



二进制特征: EB 10 66 62 3A 43 2B 2B 48 4F 4F 4B 90

第一个 API 调用,GetModuleHandIA、

API 调用 IAT 时,采用模式是 FF25

地址		数加		反汇编	注释
00405B9C	\$-	FF25	E4814500	JMP DWORD PTR DS:[<&kernel32_GetModul	eH kernel3
00405BA2		ឧឧ୮១		MOV EAX,EAX	
00405BA4	\$-	FF25	E0814500	JMP DWORD PTR DS:[<&kernel32.LocalAll	oc: kerne13
00405BAA		8BC 0		MOV EAX,EAX	
00405BAC	\$-	FF25	DC814500	JMP DWORD PTR DS:[<&kernel32.TlsGetVa	lu kernel3
LAGI AFRAG		0000		1000 EAU EAU	

2. 区段名称 分的比较细



3. 链接器版本

5.0

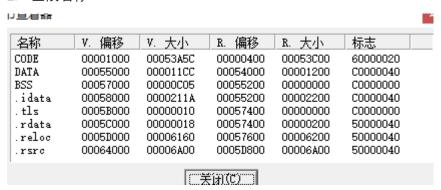
分析 Delphi 程序特征

1. OEP 特征

4.014TF	 XAJ/H		1111+
00454A14	\$ 55	PUSH EBP	
00454A15	8BEC	MOV EBP,ESP	
00454A17	83C4 F0	ADD ESP,-0x10	
00454A1A	B8 34484500	MOV EAX,Delphi7.00454834	UNICODE ";"
00454A1F	E8 3C12FBFF	CALL Delphi7.00405C60	
00454A24	A1 58604500	MOV EAX,DWORD PTR DS:[0x456058]	
00454A29	8B00	MOV EAX,DWORD PTR DS:[EAX]	
00454A2B	E8 ACE5FFFF	CALL Delphi7.00452FDC	
00454A30	8B0D 3C61450	MOV ECX,DWORD PTR DS:[0x45613C]	Delphi7.00457BFC
00454A36	A1 58604500	MOV EAX,DWORD PTR DS:[0x456058]	-
00454A3B	8B00	MOV EAX,DWORD PTR DS:[EAX]	
00454A3D	8B15 7C45450	MOV EDX,DWORD PTR DS:[0x45457C]	Delphi7.004545C8
00454A43	E8 ACESFFFF	CALL Delphi7.00452FF4	-
00454A48	A1 58604500	MOV EAX,DWORD PTR DS:[0x456058]	
00454A4D	8B00	MOV EAX,DWORD PTR DS:[EAX]	
00454A4F	E8 20E6FFFF	CALL Delphi7.00453074	
00454A54	E8 03F3FAFF	CALL Delphi7.00403D5C	
00454A59	8D40 00	LEA EAX,DWORD PTR DS:[EAX]	
BOLELAED	0000	ARR BUTE BER RO-FEAUT AL	I
$\Gamma \wedge \cap \Lambda$	γ- γ	T T A D I THE TO A T A T A T A T A T A T A T A T A T	

5 个 CALL,第一个 CALL 内有 API 调用,GetModuleHandIA

2. 区段名称



3. 链接器版本

2.25

分析 VS 程序

以链接器版本为例,分析 VC 程序

VC6.0 6.0 7.0, 7.1 VC2003 VC2005 8.0 VS2008 9.0 VS2010 10.0 VS2012 11.0 VS2013 12.0 VS2015 14.0 VS2017 14.1

分析 vc6.0 和易语言

OEP

地址	HEX	反汇编		^
0044848D	г\$	PUSH EBP		
0044848E		MOV EBP,ESP		
00448490	۱.	PUSH -0x1		
00448492	۱.	PUSH 易语言.0046E818		
00448497	۱.	PUSH 易语言.0046E818 PUSH 易语言.0044CCBC	SE	
00448490	۱.	MOV EAX,DWORD PTR FS:[0]		
004484A2	۱.	PUSH EAX		
004484A3	۱.	MOV DWORD PTR FS:[0],ESP		
004484AA	-	SUB ESP,0x58		
004484AD		PUSH EBX		
004484AE	۱.	PUSH ESI		
004484AF	۱.	PUSH EDI		
004484B0	۱.	MOV [LOCAL.6],ESP		
004484B3	۱.	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	ker	
004484B9	۱.	XOR EDX,EDX		
004484BB		MOV DL,AH		
UUTTYRED		MUN UMUKU BIK UZ.LUATOTUCUJ EUX	1	

申请局部空间是: sub esp,0x58 第一个 API 调用是 GetVersion