MEW 1.2 Manual Unpacking Uccidiamo questo gattino >:)		
Data	by evo	
2/02/2006	***UIC's Home Page***	**Published by Quequero**
Every time i look in your eyes	*Grazie evo!*	*Every day i'm watching you die*
...	**E-mail:** evobboy@yahoo.it **irc: evobboy irc.azzurra.net:6667 #crack-it**	...
Difficoltà	(X)**NewBies** ( )**Intermedio** ( )**Avanzato** ( )**Master**	

Introduzione

Si sono sempre io ev0 ma quello zero in fondo cominciava a darmi fastidio...
Meno male che questo almeno non è un'animale corazzato :D...
miaoooo*** *Bang! *evo has killed the cat...

Oggi ci occuperemo di fare il manual unpacking di questo packer, date le mie ancora scarse conoscenze su formato PE e compagnia (recentemente acquisite) spero almeno sia capibile, certamente non credo che andremo a fare una analisi completa del packer quindi rilassatevi sarà un cosa veloce e indolore ... :)

Tools usati

OllyDbg
ImportReconstructor 1.6
ProcDump

URL o FTP del programma

Northfox GDI demo 2: http://northfox.uw.hu | http://northfox.dyn.hu

Essay

Analizziamo il file con PEid, Meeeeewww =)

L'Entry Point è a 00020998h

Vediamo le sezioni del PE...

```
->Section Header Table
1. item:
Name: MEW
VirtualSize: 0x00018000
VirtualAddress: 0x00001000
SizeOfRawData: 0x00000000
PointerToRawData: 0x00000000
PointerToRelocations: 0x00000000
PointerToLinenumbers: 0x00000000
NumberOfRelocations: 0x0000
NumberOfLinenumbers: 0x0000
Characteristics: 0xC00000E0
(CODE, INITIALIZED_DATA, UNINITIALIZED_DATA, READ, WRITE)

2. item:
Name: ÒuÛŠëÔ
VirtualSize: 0x00016000
```

```
VirtualAddress: 0x00019000
SizeOfRawData: 0x000079B1
PointerToRawData: 0x00000200
PointerToRelocations: 0x00000000
PointerToLinenumbers: 0x00000000
NumberOfRelocations: 0x0000
NumberOfLinenumbers: 0x0000
Characteristics: 0xC00000E0
(CODE, INITIALIZED_DATA, UNINITIALIZED_DATA, READ, WRITE)
```

Il nostro EP cade nella seconda sezione. Guardiamo la prima, MEW: SizeOfRawData: 0x00000000, PointerToRawData: 0x00000000, bene possiamo immaginare che o stà li solo per non fare niente o ci verrà unpackato qualcosa all'interno durante il processo di unpacking...
Adesso carichiamo in Olly. Entry Point Alert! Ok lo sappiamo... Alla domanda Do you want to continue analysis? premiamo No.

```
00420998 >-E9 B7F7FDFF JMP GDI_DEMO.00400154
```

Premiamo subito F8 e ci ritroviamo nel codice del packer:

```
00400154 BE 1C904100 MOV ESI,GDI_DEMO.0041901C
00400159 8BDE MOV EBX,ESI
0040015B AD LODS DWORD PTR DS:[ESI]
0040015C AD LODS DWORD PTR DS:[ESI]
0040015D 50 PUSH EAX ;cosa verra mai pushato?
0040015E AD LODS DWORD PTR DS:[ESI]
0040015F 97 XCHG EAX,EDI
00400160 B2 80 MOV DL,80
```

cominciamo a steppare sempre con F8 (no non ve lo dico cosa è che viene pushato :) se quello è un buffer e lui unpacka a partire da lì... pensa un po che cosa è)

```
00400197 D1E8 SHR EAX,1
00400199 74 2F JE SHORT GDI_DEMO.004001CA
0040019B 13C9 ADC ECX,ECX
0040019D EB 1A JMP SHORT GDI_DEMO.004001B9
0040019F 91 XCHG EAX,ECX

;-----------------------------------
;taglio per questioni di spazio :)
;-----------------------------------

004001C3 2BF0 SUB ESI,EAX
004001C5 F3:A4 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
004001C7 5E POP ESI
004001C8 ^EB 9B JMP SHORT GDI_DEMO.00400165
004001CA AD LODS DWORD PTR DS:[ESI]
004001CB 85C0 TEST EAX,EAX
004001CD ^75 90 JNZ SHORT GDI_DEMO.0040015F
004001CF E8 400A0200 CALL GDI_DEMO.00420C14
004001D4 AD LODS DWORD PTR DS:[ESI]
004001D5 96 XCHG EAX,ESI
```

Il secondo salto evidenziato torna all'inizio di un mega loop, guardando i vari jump ci accorgiamo che ce ne è uno proprio a 4001CA (quello evidenziato in blu) quindi mettiamo un breakpoint su 4001CA, premiamo F9 (run) e incrociamo le dita, si abbiamo visto giusto.
Azz ma c'è un jnz subito dopo, e salta ancora più sù, continuiamo a tracciare e controlliamo che non faccia niente di strano, ritorniamo sempre allo stesso punto, bene :) mettiamo un bp a 4001CF e premiamo F9 (lì dove è evidenziato in verde) sempre con F8 saltate questa call, e continuiamo a steppare...

```
004001D4 AD LODS DWORD PTR DS:[ESI]
004001D5 96 XCHG EAX,ESI
004001D6 AD LODS DWORD PTR DS:[ESI]
004001D7 97 XCHG EAX,EDI
004001D8 56 PUSH ESI
004001D9 AC LODS BYTE PTR DS:[ESI]
004001DA 3C 00 CMP AL,0
004001DC ^75 FB JNZ SHORT GDI_DEMO.004001D9
004001DE FF53 F0 CALL DWORD PTR DS:[EBX-10] ;Qui viene chiamata LoadLibraryA
004001E1 95 XCHG EAX,EBP
004001E2 56 PUSH ESI
004001E3 AD LODS DWORD PTR DS:[ESI]
004001E4 0FC8 BSWAP EAX
004001E6 40 INC EAX
004001E7 59 POP ECX
004001E8 ^74 EC JE SHORT GDI_DEMO.004001D6
004001EA 79 07 JNS SHORT GDI_DEMO.004001F3
004001EC AC LODS BYTE PTR DS:[ESI]
004001ED 3C 00 CMP AL,0
004001EF ^75 FB JNZ SHORT GDI_DEMO.004001EC
004001F1 91 XCHG EAX,ECX
004001F2 40 INC EAX
004001F3 50 PUSH EAX
004001F4 55 PUSH EBP
004001F5 FF53 F4 CALL DWORD PTR DS:[EBX-C] ;Qui invece GetProcAddress
004001F8 AB STOS DWORD PTR ES:[EDI]
004001F9 85C0 TEST EAX,EAX
004001FB ^75 E5 JNZ SHORT GDI_DEMO.004001E2
004001FD C3 RETN
004001FE 0000 ADD BYTE PTR DS:[EAX],AL
00400200 0000 ADD BYTE PTR DS:[EAX],AL
00400202 0000 ADD BYTE PTR DS:[EAX],AL
```

Se avete notato da 4001CF fino a 40001FB carica le varie dll e le funzioni importate :)
Mettete un bp sul RETN, e cosa c'è nello stack? ehi ma quello non è il puntatore a quel "buffer" dove è stato unpackato tutto?
Si, e il RETN viene usato come salto all'entry point originale. Premete ancora una volta F8 e vi ritroverete all'entry point originale, dumpate con qualsiasi cosa vogliate (ProcDump, OllyDump [Senza usare rebit.dll by yoda]) e con un pe editor modificate l'entry point con quello che abbiamo trovato noi. Ricostruite le Import con Import Reconstructor attacandolo al processo corrente, mettete come OEP quello che abbiamo trovato (4F3C) premete IAT Auto Search, sono tutte import valide. Fix Dump e il nostro exe è dumpato.

evo...entuale firmetta

Note finali

Siamo arrivati alla fine, con qualche perplessità forse... ma il file è lì e funziona.
Spero solo di essere stato chiaro. =)

Un saluto a GeO, Syx, a85k, Quequero, Andreageddon, Pnluck, ZeroG, tutti gli altri di cui non ricordo il nome,
un ringraziamento di dovere anche a chiunque abbia scritto tutorial su PE e Import Table.
Acknowledgements fly out to Northfox for his packer and his gdi demo ;)

Disclaimer

portare avanti per fornire ai rispettivi consumatori i migliori prodotti possibili.

Reversiamo al solo scopo informativo e per migliorare la nostra conoscenza del linguaggio Assembly.