

كيفه تحول من RVA الى Offset يدويا ثم باستعمال ادوات

RVA to Offset : HOW TO

الجزء الأول (نظري)

by Zool@nder

1 - الفهرست:

تعريفات

العنوان النصي الافتراضي

العنوان الافتراضي

الوفسيه

كيفيه التعامل و التحويل بين قيم VA, RVA و Offset

VA --> RVA و العكس:

الطريقه الاولى لتحويل VA --> Offset :

الطريقه الثانيه لتحويل VA --> Offset :

الطريقه الثالثه لتحويل VA --> Offset :

المراجع

هناك العديد من الاعضاء الذين يجدون مشكلا في التحويل بين العنوان النسبي الافتراضي و الـ offset و لا بأس ان نبتدأ ببعض التعريفات لرفع اي لبس. فما الفرق بين VA, RVA و Offset؟

2 - تعريفات:

2.1 - العنوان النسبي الافتراضي (RVA) :

نتكلم عن الـ RVA فقط عندما يكون الملف محملا في الذاكرة. فحين يحمل لودر الـ ويندوز اي ملف PE الى الذاكرة فـ و يفعل ذلك نسبة الى قيمة محددة مسبقا في PE header و هي الـ ImageBase (هناك حالات يحمل فيها الملف التنفيذي الى عنوان مخالف للـ ImageBase). هذه النسبية هي الاساس للتحديث عن RVA و عدم استعمال عناوين ثابتة.

و اختصارا نقول: الـ RVA هي القيمة التي تصف لنا عنوانا ما, دون معرفة الـ imageBase.

و لنعتبر مثلا ملفا تنفيذا محملا في الذاكرة انطلاقا من العنوان 0x400000:

اذا اعتبرنا ان الكود سيكشن تبتدأ من 0x401000 فستكون بذلك RVA للكود سيكشن هي :

$$RVA = 0x1000 = 0x401000 - 0x400000.$$

$$0x1000(RVA) = (load\ address)0x400000 - (target\ address)^1$$

و في الاتجاه المعاكس, اذا اعتبرنا ان 0xF514 هي RVA البداية فسيكون بذلك العنوان (VA : انظر تحت) هو:

$$0xF514 + 0x400000 = 0x40F514.$$

2.2 - العنوان الافتراضي (VA) :

العنوان الافتراضي هو العنوان كما تراه في أولي و يعتبر كـ $RVA + ImageBase$. و لهذا فلا يمكن استعمال الـ VA كعناوين الا مع لودر, بينما لا تستعمل في حالة الباتشينغ او التغيير بمحرر هيكس.

2.3 - الـ offset (Offset) :

هو القيمة المميزة لبايتات الملف على القرص الصلب (و ليس في الذاكرة) و هو الاكثر استعمالا في التعامل مع الملفات التنفيذية من تعديل و زيادة و نقصان (و كمثال : محرر الهيكس لا يتعامل الا مع الـ offset).

3 - كيفية التعامل و التحويل بين قيم VA, RVA و Offset:

3.1-التحويل من VA --> RVA و العكس:

هذا اسهل التحويلات و يكفي تذكر المعادلة التالية :

$$VA = RVA + ImageBase$$

3.2- التحويل Offset --> VA (الطريقة الاولى):

و هذا بيت القصيد من هذا ا لدرسو ان شاء الله ب عد قراء ته يزول ا للبس الح اصل ع ند اغلب المبتدئين.

و سأبدأ بالمعادلة التي تحكم هذا التحويل و هي التالية:

نعتبر Target هو البايث الذي نريد تمييزه (اذكر ان لهذا البايث اوفسيت يميزه على القرص الصلب و RVA تميزه في الذاكرة)

نعتبر Target_OFFSET هو الاوفسيت الذي نريد البحث عنه و Target_RVA هو RVA التي حصلنا عليها من خلال اولي.

و نعتبر Section_OFFSET هو اوفسيت السيكتشن التي ينتمي اليها ال Target.

و اخيرا نعتبر Section_RVA هي RVA السيكتشن التي ينتمي اليها Target.

المعادلة ستكون :

$$Target_OFFSET = Target_RVA - Section_RVA + Section_OFFSET$$

او

$$Target_OFFSET = Target_VA - Section_VA + Section_OFFSET$$

و السبب من كون المعادلتين متساويتن رياضي محض و لا اظن انه يحتاج الى شرح.

كنت قد كتبت فقرتين هنا اشرح فيهما اصل هذه المعادلة, لكنني رأيت ان الامور ستصبح اكثر تعقيدا للمبتدئين, و ربما اسقط في عكس ما اردت و هو التوضيح, لذا حذفتهما و قررت وضع مثال عملي اتمنى ان تصل من خلاله الفكرة.

و لنبدأ المثال بتحميل اي ملف تنفيذي الى أولي :

و ليكن برنامج الوينرار

Address	Hex dump	Disassembly	Comment
004758DA	8D85 ACBF	LEA EAX, DWORD PTR SS:[EBP-454]	
004758E0	E8 CF15	CALL WinRAR.00466EB4	
004758E5	8D85 ACBF	LEA EAX, DWORD PTR SS:[EBP-454]	
004758EB	33D2	XOR EDX, EDX	
004758ED	E8 4A20	CALL WinRAR.0046793C	
004758F2	833D CCA1	CMP DWORD PTR DS:[4BA1CC], -1	
004758F9	0F95C1	SETNE CL	
004758FC	83E1 01	AND ECX, 1	
004758FF	84C9	TEST CL, CL	
00475901	74 0C	JE SHORT WinRAR.0047590F	
00475903	B8 B8A04B	MOV EAX, WinRAR.004BA0B8	
00475908	33D2	XOR EDX, EDX	
0047590A	E8 8D78	CALL WinRAR.0047D19C	
0047590F	68 78174A	PUSH WinRAR.004A1778	Arg2 =
00475914	68 000400	PUSH 400	Arg1 =
00475919	8D8D AC3F	LEA ECX, DWORD PTR SS:[EBP-C54]	
0047591F	BA 1B1A4A	MOV EDX, WinRAR.004A1A1B	ASCII
00475924	B8 251A4A	MOV EAX, WinRAR.004A1A25	ASCII
00475929	E8 5600	CALL WinRAR.00465984	WinRAR
0047592E	68 000400	PUSH 400	Count

و سأفترض اننا نريد تحويل العنوان الافتراضي الذي يتوقف عنده اولي في الصورة الى offset (العنوان بالاسود).

- اولاً انقل VA العنوان و هي 0x475901 (اي ان ال RVA هي 0x75901)
- ثانياً : اصعد بأولي الى اول سطر لترى VA السيكلشن 0x00401000. أي ان السيكلشن هي 0x1000.

Address	Hex dump	Disassembly	Comment
00401000	EB 10	JMP SHORT WinRAR.00401012	
00401002	66	DB 66	CHAR '6'
00401003	62	DB 62	CHAR '2'
00401004	3A	DB 3A	CHAR 'A'
00401005	43	DB 43	CHAR '3'
00401006	2B	DB 2B	CHAR 'B'
00401007	2B	DB 2B	CHAR 'B'
00401008	48	DB 48	CHAR '8'
00401009	4F	DB 4F	CHAR 'F'
0040100A	4F	DB 4F	CHAR 'F'
0040100B	4B	DB 4B	CHAR 'B'
0040100C	90	NOP	
0040100D	E9	DB E9	
0040100E	B814900	DD OFFSET WinRAR.___CPPdebugHook	
00401012	A1 A78149	MOV EAX, DWORD PTR DS:[4981A7]	
00401017	C1E0 02	SHL EAX, 2	
0040101A	A3 AB8149	MOV DWORD PTR DS:[4981AB], EAX	ntdll.
0040101F	52	PUSH EDX	
00401020	6A 00	PUSH 0	
00401022	E8 616409	CALL <JMP.<KERNEL32.GetModuleHandleA	GetModu

- ثالثاً العنصر الثالث في المعادلة و هو Section_OFFSET و يمكن اخذه مباشرة من اولي او من محرر PE. و سأختاره من أولي الان على ان نأخذه من المحرر في المثال الثاني:
الان اضغط ALT+M لرؤية نافذة الذاكرة:

[Memory map]

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapper
003A0000	00001000				Priv	RW	RW	
003B0000	00001000				Priv	RW	RW	
003C0000	00002000				Map	R	R	
003D0000	00002000				Map	R	R	
003E0000	00001000				Priv	RWE	RWE	
003F0000	00001000				Priv	RWE	RWE	
00400000	00001000	WinRAR		PE header	Imag	R	RWE	
00401000	00097000	WinRAR	.text	code	Imag	R	RWE	
00498000	00049000	WinRAR	.data	data	Imag	R	RWE	
004E1000	00001000	WinRAR	.tls		Imag	R	RWE	
004E2000	00001000	WinRAR	.rdata		Imag	R	RWE	
004E3000	00003000	WinRAR	.idata	imports	Imag	R	RWE	
004E6000	00001000	WinRAR	.edata	exports	Imag	R	RWE	
004E7000	00003000	WinRAR	.rsrc	resources	Imag	R	RWE	
00520000	00005000				Map	R E	R E	
005E0000	00002000				Map	R E	R E	
005F0000	00103000				Map	R	R	
00700000	0009E000				Map	R E	R E	
00A00000	00020000				Priv	RW		
00E00000	00001000				Map	RW	RW	
00E10000	00001000				Map	R	R	\Device

Command:

- ثم انقر مرتين على PE header المؤشر عليه في الصورة السابقة، ستفتح لك نافذة جديدة فيها جميع المعلومات عن ال PE header و منها سنأخذ المعلومة الاخيرة التي سنحتاجها. ما عليك الا ان تنزل الى تحت حتى تصل المعلومات الخاصة بال sections:

[Dump - WinRAR 00400000..00400FFF]

004002E4	00000000	DD 00000000	Delay Import Descriptor size = 0
004002E8	00000000	DD 00000000	COM+ Runtime Header address = 0
004002EC	00000000	DD 00000000	Import Address Table size = 0
004002F0	00000000	DD 00000000	Reserved
004002F4	00000000	DD 00000000	Reserved
004002F8	2E 74 65 7	ASCII ".text"	SECTION
00400300	00700900	DD 00097000	VirtualSize = 97000 (618496.)
00400304	00100000	DD 00001000	VirtualAddress = 1000
00400308	006C0900	DD 00096C00	SizeOfRawData = 96C00 (617472.)
0040030C	00060000	DD 00000600	PointerToRawData = 600
00400310	00000000	DD 00000000	PointerToRelocations = 0
00400314	00000000	DD 00000000	PointerToLineNumbers = 0
00400318	0000	DW 0000	NumberOfRelocations = 0
0040031A	0000	DW 0000	NumberOfLineNumbers = 0
0040031C	20000060	DD 60000020	Characteristics = CODE EXECUTEIF
00400320	2E 64 61 7	ASCII ".data"	SECTION
00400328	00900400	DD 00049000	VirtualSize = 49000 (299008.)
0040032C	00800900	DD 00098000	VirtualAddress = 98000
00400330	00CE0000	DD 0000CE00	SizeOfRawData = CE00 (52736.)
00400334	00720900	DD 00097200	PointerToRawData = 97200
00400338	00000000	DD 00000000	PointerToRelocations = 0
0040033C	00000000	DD 00000000	PointerToLineNumbers = 0
00400340	0000	DW 0000	NumberOfRelocations = 0

Command:

RVA السيكلشن
التي ينتمي اليها ال Target و
عرفناها من خلال قيمتها
المساوية ل 0x1000

Section_OFFSET
=
600

و لا يبقى الان الا تطبيق المعادلة و الحصول على الالوفسيت الذي نبحث عنه:
و اليكم المعلومات مجموعة :

```
1 Target_OFFSET = ????????
2 Target_RVA = 475901
3
4 Section_RVA = 401000
5 Section_OFFSET = 600
6
7 Target_OFFSET = Targer_VA - Section_VA + Section_OFFSET
8               = 475901 - 401000 + 600
9               = 74F01
10
11 الارفام كلها بالهيكس
12
```

Ln 9 : 12 Col 34 Sel 0 287 Bytes ANSI CR+LF INS Default Te

3.3- التحويل Offset --> VA (الطريقة الثانية):

في هذه الحالة سنستعمل محرر PE و لنختار LordPE

- افتح نفس الملف بالمحرر :

Basic PE Header Information

EntryPoint:	00001000	Subsystem:	0002	...
ImageBase:	00400000	NumberOfSections:	0007	
SizeOfImage:	00118000	TimeDateStamp:	43463A3E	
BaseOfCode:	00001000	SizeOfHeaders:	00001000	? +
BaseOfData:	00098000	Characteristics:	010F	...
SectionAlignment:	00001000	Checksum:	00000000	?
FileAlignment:	00000200	SizeOfOptionalHeader:	00E0	
Magic:	010B	NumOfRvaAndSizes:	00000010	+ -

OK
Save
Sections
Directories
FLC
TDSC
Compare
L

- اضغط الزر sections:

[Section Table]					
Name	VOffset	VSize	ROffset	RSize	Flags
.text	00001000	00097000	00000600	00096C00	60000020
.data	00098000	00049000	00097200	0000CE00	C0000040
.tls	000E1000	00001000	000A4000	00000200	C0000040
.rdata	000E2000	00001000	000A4200	00000200	50000040
.idata	000E3000	00003000	000A4400	00002800	40000040
.edata	000E6000	00001000	000A6C00	00000200	40000040
.rsrc	000E7000	00031000	000A6E00	00030600	40000040

Section_RVA

Section_Offset

كيف عرفنا ان هذه هي
السيكشن؟
سهل جدا، اما من Section_RVA
التي حددناها من قبل **هنا**

او
من خلال Target_RVA التي حددناها **هنا**
اذا لاحظت ان قيمتها تنتمي الى هذا
المجال

3.4- التحويل Offset --> VA (الطريقة الثالثة):

- هذه اجمل الطرق، لا حسابات و لا يحزنون، فقط ضغطة واحدة على زر و السلام ☺
- افتح ب LordPE و اضغط الزر المبين في الصورة:

Basic PE Header Information

EntryPoint:	00001000	Subsystem:	0002
ImageBase:	00400000	NumberOfSections:	0007
SizeOfImage:	00118000	TimeDateStamp:	43463A3E
BaseOfCode:	00001000	SizeOfHeaders:	00001000
BaseOfData:	00098000	Characteristics:	010F
SectionAlignment:	00001000	Checksum:	00000000
FileAlignment:	00000200	SizeOfOptionalHeader:	00E0
Magic:	010B	NumOfRvaAndSizes:	00000010

OK
Save
Sections
Directories
FLC
TDSC
Compare
L

- اضغط على الزر VA (انت الان تعرف الفرق تماما بين VA و ليس RVA)

[File Location Calculator]

Addresses

VA: **VA:**

RVA:

Offset:

DO

Additional Information

Section:

Bytes:

Hex Edit

- أدخل ال VA التي تريد تحويلها:

The screenshot shows the 'File Location Calculator' window. In the 'Addresses' section, the 'VA:' field is highlighted with a red box and contains the value '475901'. The 'RVA:' and 'Offset:' fields are empty. In the 'Additional Information' section, the 'Section:' field is empty and the 'Bytes:' field is empty. The 'DO' button is located on the right side of the window.

- أخيرا DO :

The screenshot shows the 'File Location Calculator' window. The 'DO' button is highlighted with a pink box, and a pink arrow points to it. In the 'Addresses' section, the 'VA:' field contains '00475901', the 'RVA:' field contains '00075901', and the 'Offset:' field contains '00074F01'. In the 'Additional Information' section, the 'Section:' field contains '.text' and the 'Bytes:' field contains '74 0C B8 B8 A0 4B 00 33 D2 E8'. The 'Hex Edit' button is located at the bottom right.

و ينتهي الدرس و السلام عليكم و رحمة الله و بركاته.
 اتمنى ان يكون اشكال RVA, VA and Offset قد زال الى الابد , على الاقل, نظريا و تتممة الدرس ستكون
 ان شاء الله عن كيفية التعامل برمجيا مع هذه المفاهيم.

Zool@nder|AT4RE

2007

4 - المراجع :

1. [An In-Depth Look into the Win32 Portable Executable File Format](#)
2. ["COFF "Wikipedia](#)
3. مصادر اخرى (=).