

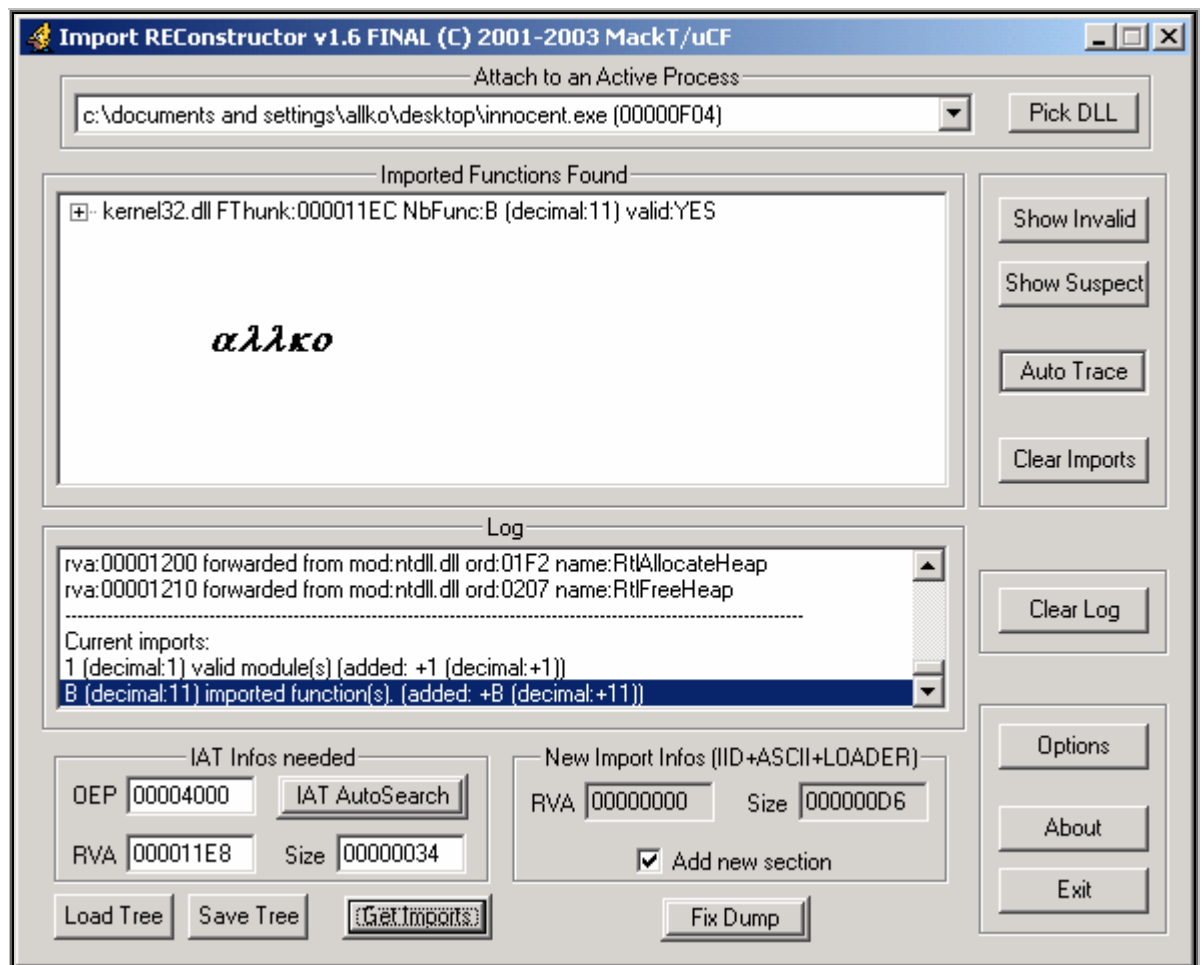
Introduction :

يتحدث درس اليوم عن أمرين...أولا سنتعلم "أسلوبا آخر" في عملية إصلاح الـ IAT (Import Address Table) للملفات المضغوطة بـ FSG ، ثانيا: كيفية فك ضغط البرامج المضغوطة بـ ASPack 2.12 يدويا . برنامج ASPack هو ضاغط ملفات متقدم ، قادر على تصغير حجم الملف لغاية 70% . إن ASPack يجعل برامج ومكتبات Windows 95/98/NT أصغر ، ويقلل زمن التحميل (download) من الانترنت أو عبر الشبكات، إضافة الى ذلك فهو يحمي البرامج من الهندسة العكسية من قبل المبتدئين .

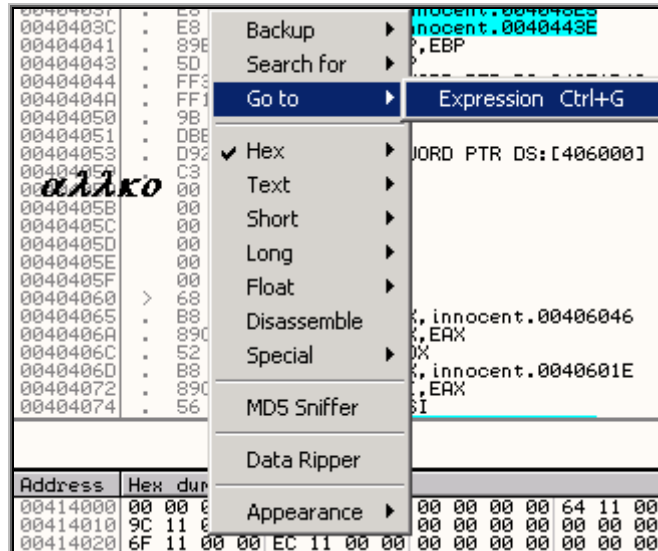
something to do with FSG

أستطيع سماعك تقول : ولماذا لم يلحق هذا الجزء بالدرس الماضي الذي هو أصلا مخصص لـ FSG بدلا من وضعه هنا ؟ الجواب : لا جواب !! إن لم يعجبك ما قمت به فنفذ الأمر التالي : jmp hell :

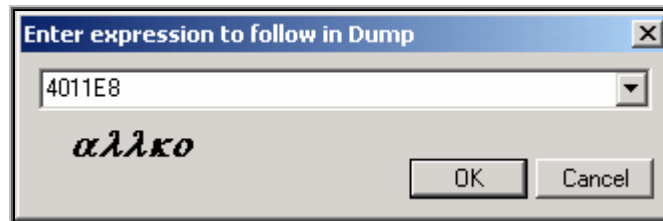
بالطبع تذكر ما فعلناه مع الضحية المسماة 2.0 في الدرس الماضي (راجع الدرس السابق)..أقصد آخر خطوة وهي توسيع نطاق البحث في ImpREC ، عندما غيرنا قيمة RVA الى 1000 وقيمة size الى 1000 ، وبدئنا بزيادة قيمة الـ size الى أن حصلنا على نتيجة صحيحة وتم إصلاح الملف (البرنامج) . ما سنقوم به اليوم هو نفس الشيء...توسيع نطاق البحث...لكن يدويا ، وبدقة أكبر... حسنا افتح الملف المسمى innocent بـ olly...ستصل الى الـ OEP (404000) ...dump ...افتح imprec...Fix Dump...GetImports...IATAutosearch...وعند تجربة الملف الناتج لن يعمل.



لكن لاحظ أن imprec قد وضع قيمة في قسم RVA... في الواقع هذه القيمة هي التي وجد عندها ال IAT الخاص بملف ال dll الذي استطاع إيجادها (تحديدا kernel32.dll)... من الواضح أن بقية ال IATs الخاصة بباقي ملفات ال dl ستكون بالقرب من من ذلك العنوان (11E8)... ما كنا نفعله هو الإبقاء على نفس العنوان لكن زيادة مدى الرؤية (أي زيادة size) وبالتالي إذا كان هناك ملفات dll أعلى أو أسفل 11E8 فسوف نجدها... لكن اليوم سنقوم يدويا بالبحث عن تلك الملفات... الأمر بسيط ، في olly في قسم Dumped Data بالأسفل اضغط باليمين واختر Go TO Expression :



سيظهر المربع التالي..اكتب عنوان ال VA الذي حصلنا عليه
 $(VA = ImageBase + RVA = 400000 + 11E8 = 4011E8)$



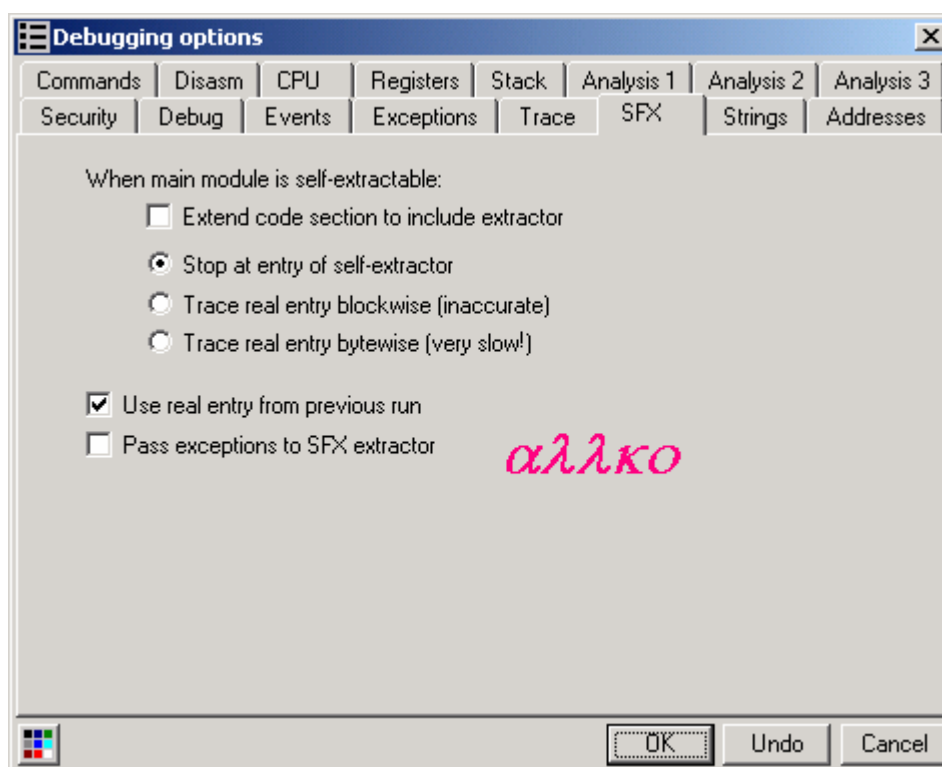
والآن قم بتكبير القسم السفلي حتى يتسنى لنا البحث بشكل جيد...

Now back to ASpack :

تجد في المرفقات برنامج ASPack . يمكنك استخدامه لضغط الملفات كي تتدرب عليها بنفسك...أيضا هناك 4 ملفات جاهزة مضغوطة به...افحص الملف target1 بـ PEiD :

ASPack 2.12 -> Alexey Solodovnikov

الآن للحصول على الـ OEP هناك طريقتان . الطريقة الأولى هي تغيير إعدادات SFX كما فعلنا في الدرس الماضي مع FSG 2.0 . إذن اذهب الى options ثم debugging options ثم اختر لسانا لتبويب SFX وغير الإعدادات الى التالي :



والآن قم بتشغيل الملف...كما تلاحظ فolly مازال يتتبع البرنامج وتختلف مدة التتبع باختلاف سرعة المعالج...عندما ينتهي من التتبع سنكون هنا :

00405EB7	. 6A 60	PUSH 60	Real entry point of SFX code
00405EB9	. 68 18564100	PUSH target1.00415618	
00405EBE	. E8 651C0000	CALL target1.00407B28	
00405EC3	. BF 94000000	MOV EDI, 94	
00405EC8	. 8BC7	MOV EAX, EDI	
00405ECA	. E8 11FBFFFF	CALL target1.004059E0	

إذن الـ OEP هي 405EB7 . الآن دعنا نرى الطريقة الثانية. أعد الإعدادات الى ما كانت عليه (أي اختر الخيار الأول بدلا من الثالث) وقم بفتح الملف. سنكون بداية هنا :

00422001	60	PUSHAD
00422002	E8 03000000	CALL target1.00422000
00422007	E9 EB045D45	JMP 459F24F7
0042200C	55	PUSH EBP
0042200D	C3	RETN
0042200E	E8 01000000	CALL target1.00422014
00422013	EB 5D	JMP SHORT target1.00422072
0042201E	BB FFFFFFFF	MOV EBX, -1

αλλκο

أول تعليمة هي PUSHAD وبالتالي نتوقع أن تكون آخر تعليمات POPAD ثم jmp الى ال OEP . لكن الحال يختلف قليلا عما قابلناه مع UPX فهناك أكثر من تعليمة POPAD وليس تعليمة واحدة... لا بأس فتعليمة PUSHAD الموجودة بالبداية لها تعليمة POPAD بالنهاية ولا يهم سواء كان هناك تعليمات من هذا النوع بين البداية والنهاية أم لا...
ما أريدك أن تعرفه هو أنه وبعد تنفيذ تعليمة PUSHAD فإن المسجلات الثمانية (بدء بـ EDI) سوف تدفع الى المكسدس... ما سنفعله هو وضع نقطة توقف على احد تلك القيم الثمانية ، وبالتالي في نهاية الروتين الخاص بال packer وعندما يصل الى تعليمة POPAD سيصل الى تلك القيمة ويتوقف لان عليها نقطة توقف...عندها نكون قد وصلنا الى نهاية روتين ال packer ونعرف أين يبدأ كود البرنامج أي نعرف ال OEP...

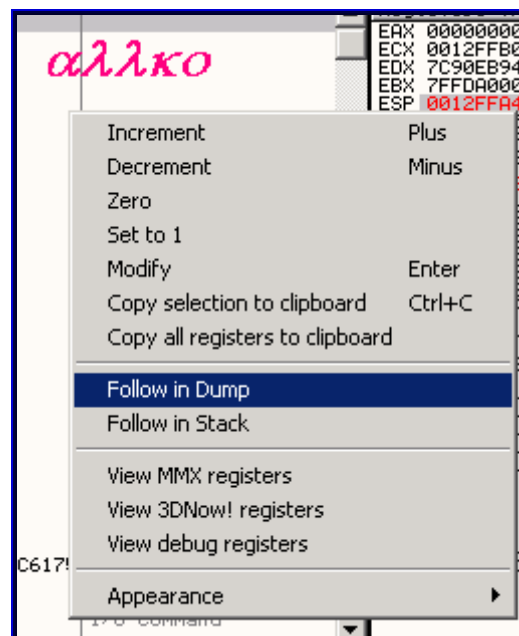
والآن قبل تنفيذ تعليمة PUSHAD لاحظ المسجلات الثمانية :

EAX	00000000
ECX	0012FFB0
EDX	7C90EB94
EBX	7FFDF000
ESP	0012FFC4
EBP	0012FFF0
ESI	FFFFFFFF
EDI	7C910738

اذن اضغط F8 ولاحظ ال stack : (لاحظ أن أول قيمة هي قيمة EDI آخر قيمة هي قيمة EAX)

0012FFA4	7C910738
0012FFA8	FFFFFFFF
0012FFAC	0012FFF0
0012FFB0	0012FFC4
0012FFB4	7FFDF000
0012FFB8	7C90EB94
0012FFBC	0012FFB0
0012FFC0	00000000

سنقوم بوضع نقطة توقف على أول قيمة وهي قيمة EDI (كما قلنا فـ EDI يدفع الى المكسدس أولا) . بجانب ESP ستجد القيمة 0012FFA4 . اضغط عليها (باليسار) كي يتم تحديدها ، والآن اضغط باليمين واختر follow in dump :



ستصل الى هنا :

Address	Hex dump	ASCII
0012FFB4	38 07 91 7C FF FF FF FF F0 FF 12 00 C4 FF 12 00	8a! = + - +
0012FFB8	00 C0 FD 7F 94 EB 90 7C B0 FF 12 00 00 00 00 00	.!26\$E! + .
0012FFC4	4F 60 81 7C 38 07 91 7C FF FF FF FF C0 FD 7F	Om!8a! + !2
0012FFD0	38 00 54 80 C8 FF 12 00 88 22 58 FF FF FF FF FF	8TC! + 2"X
0012FFE4	F3 99 83 7C 58 6D 81 7C 00 00 00 00 00 00 00	S0!Xm!.....
0012FFF4	00 00 00 00 01 20 42 00 00 00 00 00 00 00 00	...0 B....

لاحظ أول سطر...ها هي قيمة EDI (وضعت مستطيلا حولها) لكن معكوسة ...حدد أول بايتين منها (لا داعي لتحديدها كلها...) والآن اضغط على ما حددته باليمين ، ثم اختر Breakpoint ثم Hardware , on access ثم word

[illegible]

ملاحظة : جرت تحديد 4 بايتات ثم عمل نقطة التوقف على DWORD وحصلت على نفس النتيجة

والآن شغل البرنامج (F9). ها قد وصلنا إلى هنا :

004223AF	61	POPAD
004223B0	75 08	JNZ SHORT target1.004223BA
004223B2	B8 01000000	MOV EAX,1
004223B7	C2 0C00	RETN 0C
004223BA	68 B75E4000	PUSH target1.00405EB7
004223BF	C3	RETN

αλλο

ها هي تعليمة POPAD . تتبع (اضغط F8 ثلاث مرات) وستصل الى هنا :

00405EB7	6A	DB 6A	CHAR 'j'
00405EB8	60	DB 60	CHAR 'j'
00405EB9	68	DB 68	CHAR 'h'
00405EBA	18	DB 18	

لاحظ أننا حصلنا على نفس ال OEP التي حصلنا عليها بالطريقة السابقة...و كما ترى فالكود "مبهم" لأن Oally لم يقم بتحليله بعد..يمكنك - إن أردت - أن تزيل الإبهام بالضغط على CTRL+A لتحليله وستحصل على :

00405EB7	6A 60	PUSH 60
00405EB9	68 18564100	PUSH target1.00415618
00405EBE	E8 651C0000	CALL target1.00407B28
00405EC3	BF 94000000	MOV EDI,94
00405EC8	8BC7	MOV EAX,EDI
00405ECA	E8 11FBFFFF	CALL target1.004059E0
00405ECF	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP

اللكو

والآن من قائمة Plug ins اختر Olly Dump ثم Dump Debugged Process ليظهر لك :

Start Address: 400000 Size: 25000 Dump

Entry Point: 22001 -> Modify: 5EB7 Get EIP as OEP Cancel

Base of Code: 1000 Base of Data: 14000

اللكو

☒ Fix Row Size & Offset of Dump Image

Section	Virtual Size	Virtual Offset	Raw Size	Raw Offset	Characteristics
.text	00013000	00001000	00013000	00001000	C0000040
.rdata	00005000	00014000	00005000	00014000	C0000040
.data	00007000	00019000	00007000	00019000	C0000040
.rsrc	00002000	00020000	00002000	00020000	C0000040
.aspack	00002000	00022000	00002000	00022000	C0000040
.adata	00001000	00024000	00001000	00024000	C0000040

☒ Rebuild I.T using "reblt.dll" by y0da

والآن اختر Dump واحفظه بأي اسم . أبق Olly مفتوحا وشغل ImpREC . من القائمة العلوية اختر الملف الضحية وفي مربع OEP اكتب 5EB7 ثم IATauto search ثم GetImports .

Imported Functions Found	
+ comctl32.dll	FTThunk:00014000 NbFunc:1 (decimal:1) valid:YES
+ gdi32.dll	FTThunk:00014008 NbFunc:19 (decimal:25) valid:YES
+ kernel32.dll	FTThunk:00014070 NbFunc:68 (decimal:104) valid:YES
+ oleaut32.dll	FTThunk:00014214 NbFunc:3 (decimal:3) valid:YES
+ shell32.dll	FTThunk:00014224 NbFunc:1 (decimal:1) valid:YES
+ user32.dll	FTThunk:0001422C NbFunc:66 (decimal:102) valid:YES
+ winmm.dll	FTThunk:000143C8 NbFunc:6 (decimal:6) valid:YES
+ winspool.drv	FTThunk:000143E4 NbFunc:3 (decimal:3) valid:YES

اللكو

لحسن الحظ فجميع الدوال كما ترى صحيحة (انظر الى كلمة yes بجانب كل منهم) .
ملاحظة : أعتقد انك تعرف ما يجب فعله في حال كان هناك دالة أو أكثر معطوبة (NO) ... ببساطة اختر show invalid ثم اضغط باليمين على ما تم تحديده بالأزرق واختر cut Thunks .

والآن اختر Fix Dump ثم اختر الملف الذي قمنا توا بحفظه...شغل الملف...رائع أنه يعمل بنجاح !!
تجد بالمرفقات ملفا آخر (رقمه 2) يمكنك التدرب عليه فهو بنفس الفكرة تماما.
الى هنا ينتهي درسنا لهذا اليوم أمل أن تكونوا قد استفدتم واستمتعتم.

Do You Know ?

29a

مجموعة 29a هي مجموعة أسبانية (لكن بالطبع أعضاؤها من مختلف دول العالم) متخصصة في كتابة الفيروسات ، تأسست سنة 1996 ومازالت مستمر حتى الآن ، وتعد هذه المجموعة أحد أشهر المجموعات على الإطلاق... يذكر أن أول فايروس مخصص للجوالات كان قد تمت برمجته من قبل أحد أعضاء هذه المجموعة. حتى الآن قامت هذه المجموعة بنشر 8 ezines (مجلات) يمكن الحصول عليهم من موقع المجموعة على الانترنت : <http://vx.netlux.org/29a>

Outroduction :

Another easy-to-unpack packer , yet very good to learn. I hope that new concept are learned from this lesson. any comments or suggestions are welcomed. you can reach me at www.alalame.net/vb forums.

THXS :

DiDi
Dahaka
Dj-siba
Cold-Fever
alalame.net/vb members
ARTeam forums

June 2006