

Introduction :

تكلما في الدرس الماضي عن كيفية فك ضغط UPX يدويا...اليوم سنقوم بفك ضغط برنامج FSG .
FSG هو ضاغط برامج مخصص للبرامج الصغيرة الحجم (أقل من 100 كيلوبايت) ، تحديدا البرامج المبرمجة بالاسمبلي.
وهو يستخدم خوارزمية aPLib للضغط . طبعا هذا لا يعني أنه لن يستخدم للبرامج الأكبر حجما أو المبرمجة بلغات أخرى...

Here we go...

تجد في المرفقات برنامج FSG بمختلف إصداراته ، حتى تتمكن من ضغط الملفات لتختبر نفسك.

FSG 2.0

قم بفحص الملف 2.0 باستخدام PEiD .

FSG 2.0 -> bart/xt

هناك طريقتان للحصول على ال OEP وكلاهما تؤديان الى نفس النتيجة . سنبدأ بالطريقة الأولى...افتح الملف المسمى 2.0 باستخدام olly . ها نحن هنا :

00400154	8725 BCA24100	XCHG DWORD PTR DS:[41A2BC],ESP
0040015A	61	POPAD
0040015B	94	XCHG EAX,ESP
0040015C	59	PUSH EBP
0040015D	A4	MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]

انزل قليلا للأسفل...ستجد التالي :

004001CC	40	INC EAX
004001CD	78 F3	JS SHORT 1.004001C2
004001CF	75 03	JNZ SHORT 1.004001D4
004001D1	FF63 0C	JMP DWORD PTR DS:[EBX+C]

هل ترى هذه القفزات الثلاث المتتابة ؟ هذه هي العلامة المميزة لـ FSG 2.0 . ضع نقطة توقف عند القفزة الثالثة ثم F9 . والآن F7 .

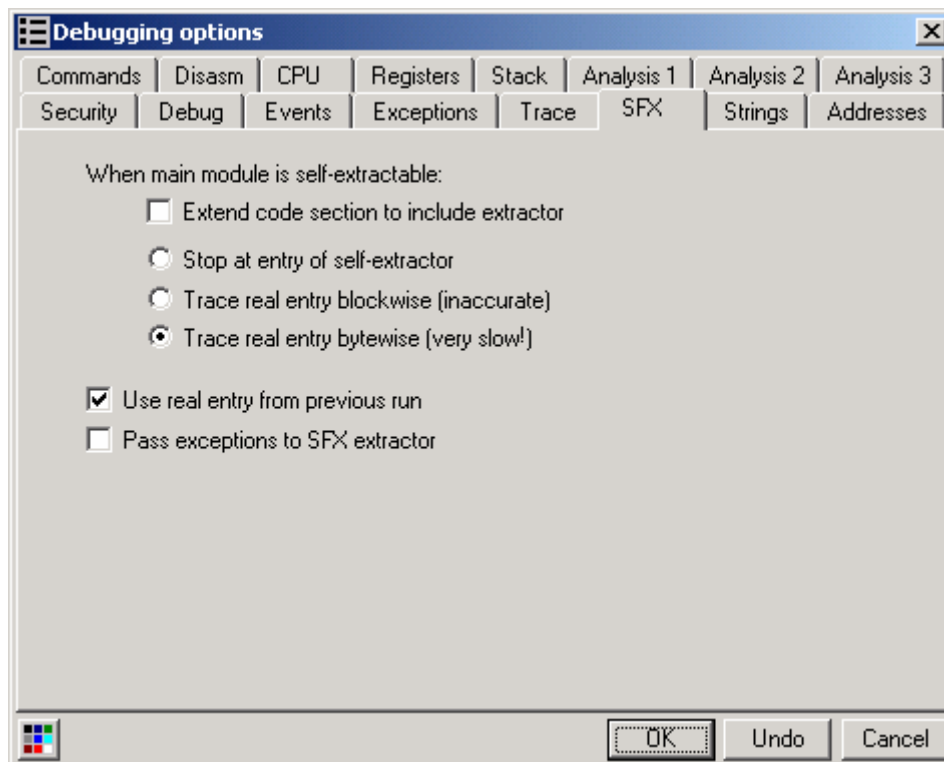
0040182E	6A	DB 6A	CHAR 'j'
0040182F	00	DB 00	
00401830	E8	DB E8	
00401831	CD	DB CD	

ها قد وصلنا ، إذن ال OEP هي 0040182E . هل ترى كم العملية سهلة...يمكنك (ليس ضروريا) أن تحلل الكود لتزيل الإبهام عن ما تراه...اضغط ctrl+A لتحصل على :

0040182E	6A 00	PUSH 0	pModule = NULL
00401830	E8 CD010000	CALL 1.00401A02	GetModuleHandleA
00401835	A3 40314000	MOV DWORD PTR DS:[403140],EAX	

(ملاحظة : في بعض الحالات عندما تصل الى هذه المرحلة ستجد أن التحليل لن يجدي نفعا وسيبقى الكود مبهما...لا بأس عندها أكمل العملية كالمعتاد ولا تهتم كثيرا)

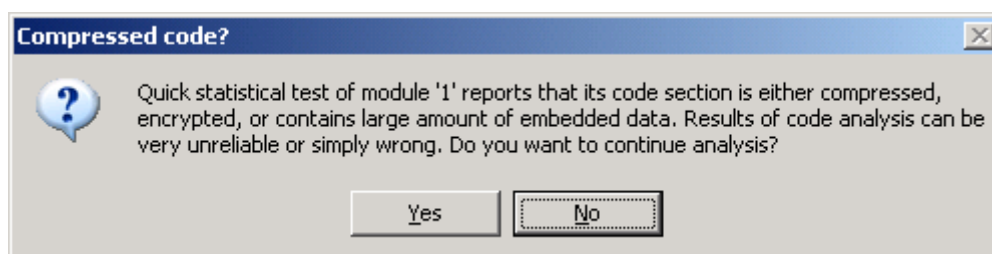
نأتي الآن الى الطريقة الثانية...فلنقم بتغيير بعض الاعدادات...من قائمة options اختر debugging options ثم من النافذة التي ستظهر اختر لسان التويب SFX وغير الاعدادات الى ما تراه بالصورة :



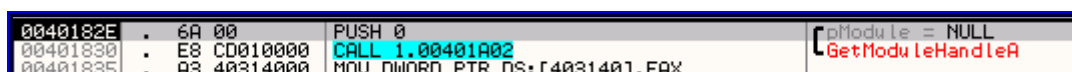
كما ترى فقد اخترنا الخيار الثالث الذي سيوفر علينا عناء البحث عن ال oep حيث سيتكفل olly بالمهمة. والآن افتح الملف...سترى في الأسفل ما يلي :

Tracing SFX: read=00401000

هذا يعني أن olly يقوم بتتبع البرنامج لذا عليك الانتظار قليلا (يختلف الوقت باختلاف سرعة المعالج لديك) . بعدما ينتهي ستخرج لك الرسالة التي تعودنا عليها :



بالطبع اختر موافق. والآن ستري التالي :



هذه هي ال OEP . لاحظ أننا حصلنا على نفس النتيجة باستخدام الطريقتين... والآن من قائمة plug اختر Olly Dump ثم Dump debugged process . ستخرج لك النافذة التالية :

Start Address: 400000 Size: 1B000 Dump

Entry Point: 154 -> Modify: 182E Get EIP as OEP Cancel

Base of Code: 1000 Base of Data: C

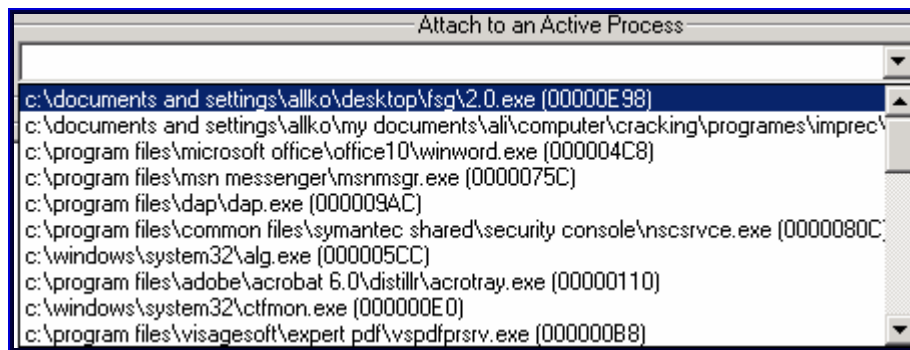
☒ Fix Raw Size & Offset of Dump Image

Section	Virtual Size	Virtual Offset	Raw Size	Raw Offset	Characteristics
	00013000	00001000	00013000	00001000	C00000E0
	00007000	00014000	00007000	00014000	C00000E0

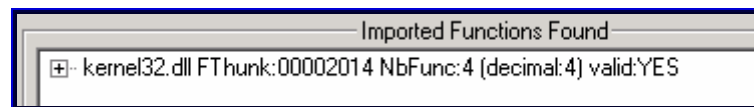
αλλκο

☒ Rebuild IT using "rebit.dll" by y0da

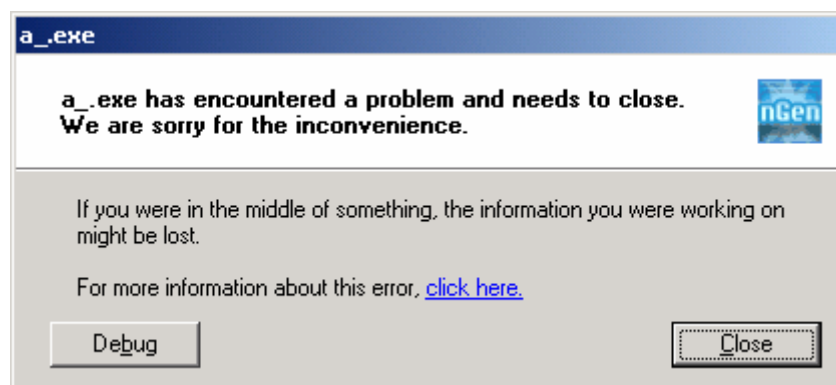
اختر Dump . بخصوص الخيار في الأسفل ، فبال تجربة ثبت لي أن وضع علامة صح أو عدم وضعها لن يؤثر . (يفترض إذا وضعنا علامة الصح أن يغنيا ذلك عن استخدام imprec ...)
والآن شغل IMPrec . من القائمة المندسلة (أم المندسلة؟ :) في الأعلى والمسماة Attach to an active process ابحث حتى تجد برنامجنا أي 2.0.exe .



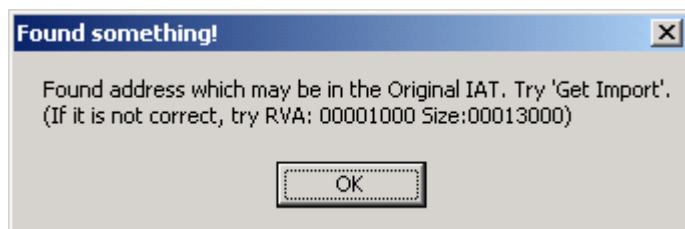
الآن في خانة OEP اكتب العنوان الذي حصلنا عليه ، أي 182E ثم اضغط IATauto search ، ستخرج لك رسالة...اضغط موافق..الآن اضغط على زر GetImports . يفترض أن يظهر لديك الصورة التالية :



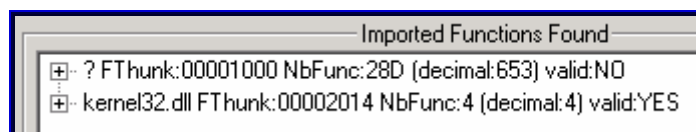
كما ترى حصلنا على ملف dll واحد فقط...الآن اضغط FixDump واختر الملف الذي قمنا بحفظه للتو في olly . قم بتشغيل الملف...



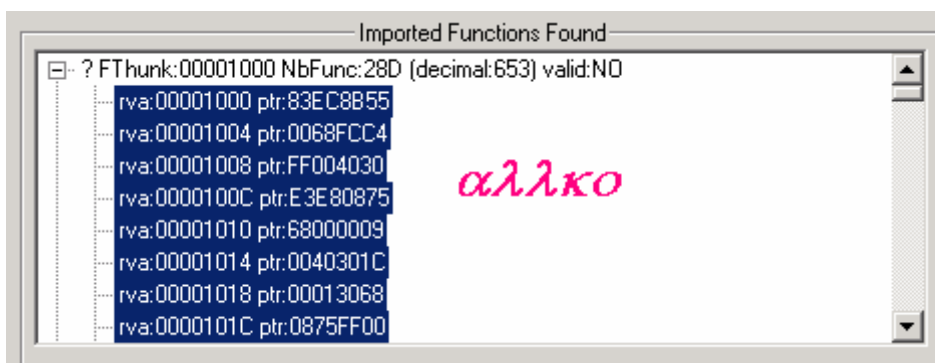
هذا ما حصلنا عليه...لماذا؟ السبب الواضح و الأكيد هو أن ال IAT ليس كاملا بعد...يبدوا أن هناك المزيد من ملفات ال dll المستوردة غير kerner32.dll . إذن ما العمل ؟ هل تذكر تلك الرسالة التي خرجت بعد الضغط على IATauto search ؟
دعني أذكرك بها :



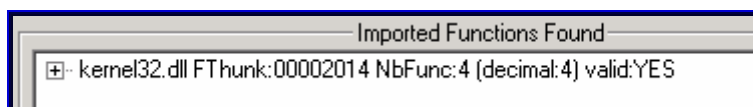
يقول ImpREC : If it is not correct , try RVA:1000 Size: 13000 . حسنا شكرا على النصيحة :) اذهب الى مربع RVA وضع القيمة 1000 ثم الى مربع Size وضع القيمة 1000 (القيمة 13000 كبيرة جدا...سنبدأ بالقيمة 1000 لأنها اصغر و أخف على الجهاز) . الآن اضغط GetImports لترى التالي :



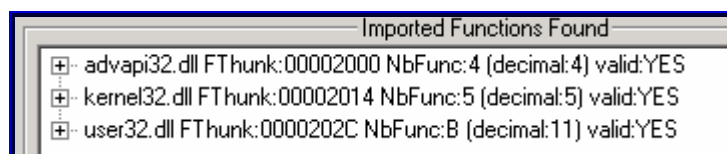
ها قد وجدنا ملف dll مستورد آخر...لكن يبدوا أنه معطوب لاحظ كلمة valid : NO . لا بأس دعنا نجرب...والآن اضغط على زر Show Invalids .



اضغط على العناوين المظلمة بالأزرق بالزر اليمين واختر Cut Thunks . هذا ما ستحصل عليه :



هذا يعني أن جميع الدوال في ذلك الملف (ملف ال dll) كانت معطوبة ولا يوجد بها أي ملف صالح...إذن فلنقم بتوسيع نطاق البحث...تذكر أن ImpRec اقترح علينا القيمة 13000 في خانة الحجم...لذلك قم بتكبير القيمة التي استخدمناها من 1000 الى 2000 . اضغط GetImports . (ستحصل على عدد كبير من الملفات...) ثم ShowInvalid ثم اضغط على العناوين المظلمة بالأزرق بالزر اليمين واختر Cut Thunks . النتيجة هي :



رائع !! حصلنا على ملفي dll مستوردين صحيحين آخرين. إذن اختر FixDump ثم اختر الملف الذي حفظناه من olly . الآن قم بتشغيل الملف...رائع!! إنه يعمل بنجاح...

قبل أن انتقل الى الإصدار الآخر من FSG...لدي ملاحظة. في بعض الأحيان تضطر الى توسيع نطاق البحث عدة مرات وقد تصل الى القيمة 5000 . لذا ، مستقبلا ، لديك الخيار إما أن تقوم بتوسيع نطاق البحث بمقدار 1000 بالمرة الواحدة أو أن تقفز الى القيمة 5000 فوراً...أنا اختار الطريقة الأولى لسبب بسيط...عندما تصل الى 5000 ، فعملية ال cutthunks ستكون مرهقة للجهاز كثيرا ، وحيث أن جهازك يعمل على معالج من العصور الوسطى (1700 mhz) لذلك فلا أحب أن أغامر من البداية فقد أحصل على النتيجة الصحيحة مع القيمة 2000 أو 3000...وإذا اضطررت فسأذهب الى الـ 5000...

FSG 1.1 , 1.2 , 1.3

بالنسبة لهذا الإصدارات فانه ما من علامة مميزة كما في الإصدار 2.0 ، لكن ببساطة استخدم الطريقة الثانية لإيجاد الـ OEP (أقصد طريقة تغيير الإعدادات) ومن ثم أكمل كالمعتاد...هذه الطريقة تنجح مع جميع الإصدارات .

Do You Know ?

سبيويه

أبو بشر عمرو بن عثمان بن قنبر، المعروف بسبيويه (فارسي: سبويه أي: "المطيب برائحة التفاح") (ح. 760 - 793) إمام نحاة العربية. ولد حوالي عام 760 في مدينة بيضاء (نساياك) في إقليم فارس، بإيران المعاصرة. ونشأ في البصرة، وتوفي في شيراز عام 793. من أول وأعظم النحاة للغة العربية. وصفه الصوتي للغة العربية هو الأدق حتى الآن. عندما كان سبيويه صغيراً يدرج مع أقرانه كان يتلقى في ربوع البصرة الفقه والحديث، وذات مرة ذهب إلى شيخه حماد البصري ليتلقى منه الحديث ويستملي منه قول النبي صلى الله عليه وسلم: «ليس من أصحابي أحد إلا ولو شئت لأخذت عليه ليس أبا الدرداء ...» فقرأه سبيويه على هذا النحو: «ليس من أصحابي أحد إلا ولو شئت لأخذت ليس أبو الدرداء ...»، فصاح به شيخه حماد: «لَحَنْتَ يا سبيويه، إنما هذا استثناء»؛ فقال سبيويه: «والله لأطلبن علماً لا يلحنني معه أحد»، ثم مضى ولزم الخليل بن أحمد وغيره. ومن هنا كانت بدايته. درج كل العلماء والباحثين والمصنفين على أن يضعوا أسماء لمؤلفاتهم ومصنفاتهم، إلا أن الوضع مع سبيويه اختلف؛ فهو لم يضع لكتابه اسماً أو حتى مقدمة أو خاتمة، ويرجح البعض أن سبب ذلك هو أنه مات في ريعان شبابه قبل أن يخرج كتابه وأخرجه عنه تلميذه أبو الحسن الأخفش إلى الوجود دون اسم؛ عرفانا بفضل أستاذه وعلمه وخدمة للغة القرآن فأطلق عليه العلماء اسم الكتاب، فإذا ذكر الكتاب مجردا من أي وصف فإنما يقصد به كتاب سبيويه.

Outroduction :

FSG is really simple packer to unpack...maybe in next lessons we could see more complicated packers...BTW , next lesson will be about ASPack 2.12...another simple packer... as usual , any suggestions , criticisms or thanks are welcomed. (my email won't be easy to get anymore...if u really want to contact me , you can find it :) .

Greetings :

DiDi , hope you do well in your exams.
Xacker : best wishes in your exams man.
Dj-Siba : keep the good work...
Cold-Fever : everyday I like you more and more :)
Saqr2002 : best wishes...thx for that good forum...place#1 for learning.