تأليف : JAAS
jaas1001@hotmail.com

الموقع : الفريق العربي للبرمجة
http://www.arabteam2000.com

الكتابة فوق الملفات التنفيذية (مبدأ عمل بعض الفايروسات)

السلام عليكم ورحمة الله
في هذا المثال سنأخذ فكرة عن الكتابة في الملفات التنفيذية مثل ماتقوم بة بعض الفايروسات والبرامج الأخرى
لاحظ الملف المرفق مع الدرس : شغل البرنامج لترى نافذة البرنامج .. يعمل بشكل طبيعي !!؟

ما رأيك لو قمنا بكتابة برنامج صغير داخل برنامج المثال ... ينفذ ما تريد .. ثم يرجع التنفيذ للبرنامج الرئيسي ويعود كما كان !
سنقوم في هذا الدرس بجعل البرنامج أول ما يشتغل يظهر رسالة (مسج) فارغة ثم يعود وينفذ محتوى الملف
شغل برنامج Olly من قائمة Fil ثم Open وإختر الملف المرفق ثم أظهر نافذة الدوال المستوردة Ctrl + N
إبحث عن دالة إظهار المسج وهي MessageBox :: أكيد ما لقيتها ؟
بإختصار البرنامج لا يتصل بدالة المسج (ولو كان يتصل بهذة الدالة لسهل العملية كثيـــــر)
والحل :
١ – سنقوم بتحميل المكتبة عن طريق الدالة LoadLibraryA وأكيد سنحمل المكتبة user32.dll لأنها تحتوي على دالة المسج
٢- سنقوم بإستخراج عنوان دالة المسج في المكتبة بإستخدام الدالة GetProcAddress
٣- ثم نتصل بعنوان دالة المسج وهي MessageBoxA لتظهر الرسالة على الشاشة

ملاحظة :
الدالتين : LoadLibraryA و GetProcAddress موجودة في أغلب البرامج حتى لو لم يكتبها المبرمج في الكود (بما فيها مثالنا) لأن أغلب المترجمات تستخدمها للتحقق من تحميل المكاتب .. ولها إستخدامات أخرى أما الفايروسات فتخزن عناوين هذة الدالتين – وتكتبها مباشرة في أي ملف تنفيذي ليتم الإتصال بها

الحين لو تجي تتصل بالدالة LoadLibraryA لوجدت أنها تطلب بارمتر واحد وهو إسم المكتبة
ونلاحظ أن إسم المكتبة عبارة عن بيانات (بمعنى أننا سنقوم بكتابة إسم المكتبة user32.dll في قسم البيانات)
والدالة الثانية تطلب بارمترين الأول عنوان المكتبة – وهذا سهل (وهو قيمة المسجل Eax بعد تنفيذ الدالة الأولى
والبارمتر الثاني إسم الدالة MessageBoxA وكما تلاحظ أن الإسم بيانات وليس كود ينفذ

أول شيء سنقوم بة كتابة البيانات الخاصة بنا في قسم البيانات :
شغل برنامج Olly ومن قائمة View ثم File وإختر الملف المرفق لفتح البرنامج داخل محرر هكس
قسم البيانات يبدأ عند عنوان x5000 توجهة لهذا العنوان ثم إنزل حتى تجد فراغ لنكتب فية البيانات الخاصة بنا بهذة الطريقة (لاحظ العنوان + البيانات)

```
00005310 81 00 81 00 81 00 81 00 01 00 01 00 01 00 01 00 ü.ü.ü.ü.☺.☺.☺.☺.
00005320 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 ☺.☺.☺.☺.☺.☺.☺.☺.
00005330 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 ☺.☺.☺.☺.☺.☺.☺.☺.
00005340 10 00 10 00 10 00 10 00 10 00 10 00 82 00 82 00 ►.►.►.►.►.►.é.é.
00005350 82 00 82 00 82 00 82 00 02 00 02 00 02 00 02 00 é.é.é.é.☻.☻.☻.☻.
00005360 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ☻.☻.☻.☻.☻.☻.☻.☻.
00005370 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ☻.☻.☻.☻.☻.☻.☻.☻.
00005380 10 00 10 00 10 00 10 00 20 00 00 00 00 00 00 00 ►.►.►.►. .......
00005390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000053A0 75 73 65 72 33 32 2E 64 6C 6C 00 00 4D 65 73 73 user32.dll..Mess
000053B0 61 67 65 42 6F 78 41 00 00 00 00 00 00 00 00 00 ageBoxA.........
000053C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000053D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000053E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000053F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00005400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00005410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

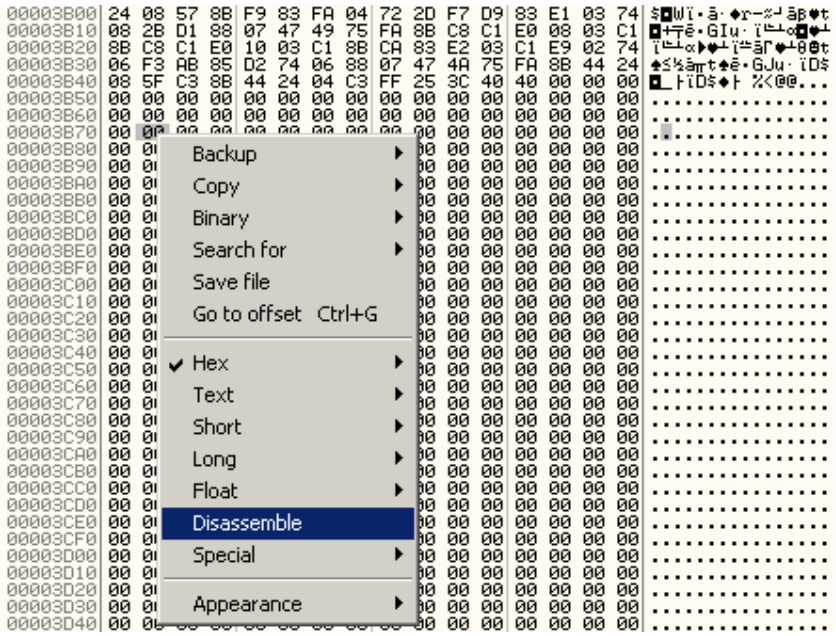
إفتح ملف نصي وخزن عنوان كل معلومة

إسم المكتبة = يوجد في العنوان x53A0 ثم نظيف لها عنوان البرنامج الوهمي ٤٠٠٠٠٠ =x4053A0
إسم الدالة =يوجد في العنوان x53AC // // // =x4053AC

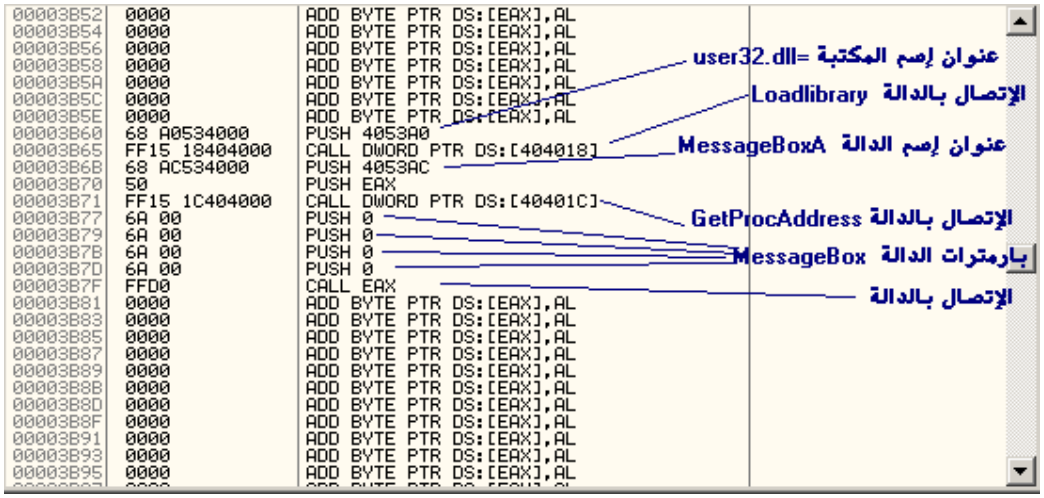
بعد أن نكتب البايانات نحتاج لعناوين الدوال التي سنتصل بها وهي LoadLibraryA و GetProcAddress
ولمعرفتها شغل نسخة ثانية من برنامج Olly ثم File ثم Open إختر مقطع الكود ونفذ Ctrl+N
وإبحث عن الدالتين لتجد عناون كل دالة بجانبها وهذة هي العناوين

KERNEL32.GetProcAddress =0040401C
KERNEL32.LoadLibraryA =00404018

أغلق النسخة الأخيرة من برنامج Olly وإرجع لمحرر الهكس لبرنامج Olly
إذهب لمقطع الكود بدايتة العنوان x1000 وإنزل إلى أن تجد الفراغ وأكتب هذا الكود
أول شيء غير طريقة العرض (من ترميز هكس إلى إسمبلي) بهذة الطريقة



ثم إكتب الكود :: عند العنوان x3B60



شرح أكثر للكود الذي قمنا بكتابتة

PUSH 4053A0
CALL DWORD PTR DS:[404018]
PUSH 4053AC
PUSH EAX
CALL DWORD PTR DS:[40401C]
PUSH 0
PUSH 0
PUSH 0
PUSH 0
CALL EAX

أول سطرين : تحميل المكتبة user32.dll بإستخدام الدالة LoadLibrary

PUSH 4053A0
CALL DWORD PTR DS:[404018]
نفس السطرين بلغة السي
LoadLibrary("user32.dll");

PUSH 4053A0 : التعليمة
معناها دفع إسم المكتبة توجه للعنوان ولاحظ إسم المكتبة
CALL : التعليمة
بمعنى إتصل بالدالة LoadLibrary

التعليمة الثانية : معرفة عنوان دالة المسج في الذاكرة بإستخدام الدالة GetProcAddress

PUSH 4053AC
PUSH EAX
CALL DWORD PTR DS:[40401C]
بلغة السي
GetProcAddress (EAX,"MessageBoxA");
والمسجل Eax يمثل القيمة العائدة من الدالة التي قبلها
بمعنى أن التعليمتين السابقتين
HMODULE mydll=LoadLibrary ("user32.dll");
GetProcAddress (mydll,"MessageBoxA");
أكيد لاحظت إن البارمترات في لغة الإسمبلي تكتب بالعكس
وللمعلومة كل العناوين تكتب بالعكس – قانون

التعليمة الثالثة : إظهار الرسالة للمستخدم بإستخدام الدالة MessageBox

PUSH 0
PUSH 0
PUSH 0
PUSH 0
CALL EAX
بلغة السي
MessageBox(NULL,NULL,NULL,NULL);

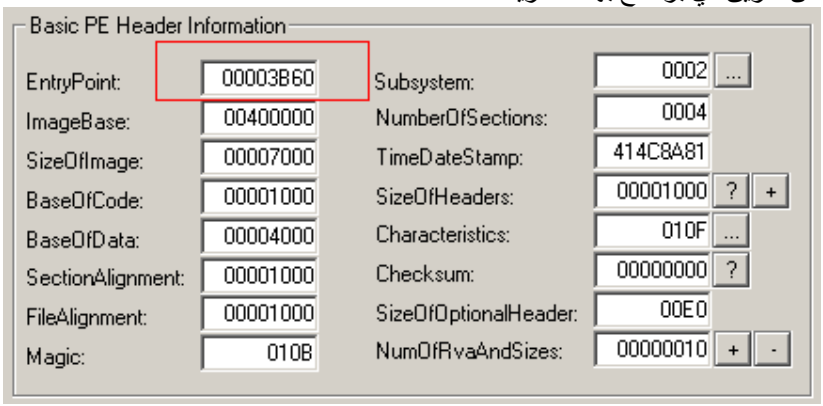
ومعناة إظهار مسج فارغ
وإذا حبيت تظهر أي رسالة إكتبها في قسم البيانات وإحفظ عنوانها
ثم إكتب العنوان في البارمتر الثاني

إلى هذة اللحظة فقد قمنا بإدخال برنامج صغير عبارة عن إظهار رسالة فارغة للمستخدم
ولكن لن ينفذ ؟! لأنة لا يوجد أمر إستدعاء لهذا الكود في البرنامج الرئيسي

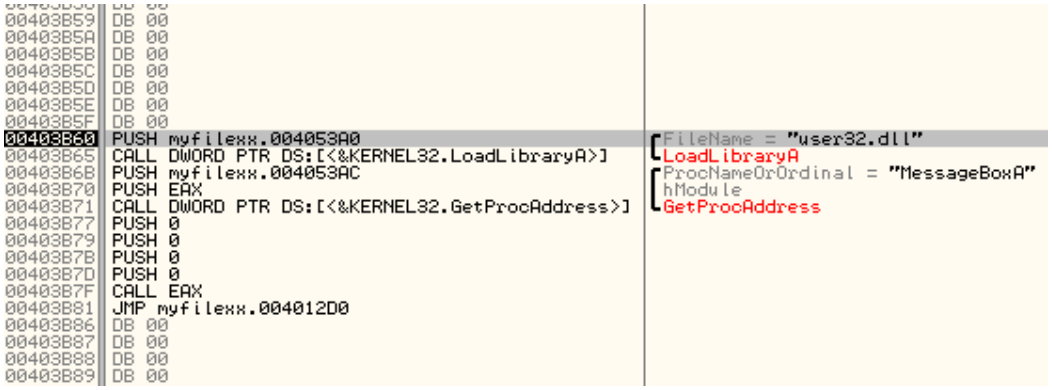
ولكي ننفذ هذا الكود ونعود للبرنامج الرئيسي -- الطريقة سهلة
أظهر عنوان بداية البرنامج وهو x12D0 (كل هذة المعلومات موجودة في ترويسة الملف التنفيذي)
والآن سنقوم بتغييرة إلى عنوان بداية برنامجنا x3B60
وبعد أن ينفذ برنامجنا سنقوم بكتابة تعليمة قفز غير مشروط JMP إلى عنوان بداية التنفيذي الحقيقي ليعود التنفيذ للبرنامج الأصلي
أضف هذة التعليمة لبرنامجنا
Jmp 12D0
ليصبح الكود بهذا الشكل

```
00003B56  0000            ADD BYTE PTR DS:[EAX],AL
00003B58  0000            ADD BYTE PTR DS:[EAX],AL
00003B5A  0000            ADD BYTE PTR DS:[EAX],AL
00003B5C  0000            ADD BYTE PTR DS:[EAX],AL
00003B5E  0000            ADD BYTE PTR DS:[EAX],AL
00003B60  68 A0534000     PUSH 4053A0
00003B65  FF15 18404000   CALL DWORD PTR DS:[404018]
00003B6B  68 AC534000     PUSH 4053AC
00003B70  50              PUSH EAX
00003B71  FF15 1C404000   CALL DWORD PTR DS:[40401C]
00003B77  6A 00           PUSH 0
00003B79  6A 00           PUSH 0
00003B7B  6A 00           PUSH 0
00003B7D  6A 00           PUSH 0
00003B7F  FFD0            CALL EAX
00003B81 ^E9 4AD7FFFF     JMP 000012D0
00003B86  0000            ADD BYTE PTR DS:[EAX],AL
00003B88  0000            ADD BYTE PTR DS:[EAX],AL
00003B8A  0000            ADD BYTE PTR DS:[EAX],AL
00003B8C  0000            ADD BYTE PTR DS:[EAX],AL
00003B8E  0000            ADD BYTE PTR DS:[EAX],AL
00003B90  0000            ADD BYTE PTR DS:[EAX],AL
```

بعد أن تكتب الكود كامل :: تأكد أنك غيرت عنوان بداية تشغيل البرنامج من العنوان x12D0 إلى x3B60
عن طريق أي برنامج بهذة الطريقة



إحفظ البرنامج بأي إسم :
ولآن شغل البرنامج ولاحظ التغييرات (سيظهر رسالة – ثم يعود للنافذة الرئيسية)
أغلق البرنامج وشغل برنامج Olly ومن File ثم Open وإختر برنامجنا لترى كود بداية التنفيذ بهذا الشكل



نفذ البرنامج خطوة خطوة F8 ولاحظ طريقة عملة (وبهذا نكود قد إنتهيناء من المثال)

معلومات أخرى :

لاحظت أننا قمنا بخطوات قد تكون كثيرة والسبب – لأننا غيرنا في الملف بطريقة يدوية
ولو أردنا التغيير عن طريق برنامج (مثل عمل الفايروسات والبرامج الأخرى فالطريقة ستكون أسهل)
لاحظت في مثالنا أننا قمنا بإستدعاء دالتين LoadLibrary و GetProcAddress وهذة الدوال فقط لإستخراج
عنوان المسج وكتابتة في البرنامج ؟

أما الفايروسات فلا تقوم بهذة الخطوة داخل البرنامج لأسباب منها :
١- يمكن الدوال ما تكون موجودة في الملف الذي تكتب علية
٢- تصغير حجم الكود الذي ستكتبة
نفس مثالنا هذا لو أردنا كتابتة في برنامج ولنفترض أنة فايروس
فنكتب داخل الفايروس هذة الدوال LoadLibrary و GetProcAddress
ثم نكتب في البرنامج الضحية فقط إتصال بالقيمة المعادة من الدالة GetProcAddress
لنفرض أن القيمة المعادة = ٧٨٩٩٩٦
فيصبح البرنامج الذي كتبناة بهذا الشكل

```
PUSH 0
PUSH 0
PUSH 0
PUSH 0
CALL 789996
Jmp 12D0
```

بهذة الطريقة سيعمل نفس البرنامج (لاحظ أننا لم نعتمد على أي دالة داخل البرنامج + صغرنا حجم الكود)

النقطة الثانية :
لو أردنا كتابة برنامج كبير داخل البرنامج ولم تكفي الفراغات لكتابة الكود ؟
الحل في هذة الطريقة سهل ؟!
نقوم بإنشاء قسم جديد بخصائص الكود + البيانات
ونكتب بة كل البيانا والكود - ثم نغير بداية تنفيذ البرنامج إلى عنوان القسم الذي أنشأناة
وبهذة الطريقة نكون أضفنا برنامج كامل إلى البرنامج الأصلي

هذا والله أعلم