



Remember Me ☐ User Name User Name
 Password

PersianTools Forums > برنامه نویسی و طراحی وب، سیستمهای مدیریت سایت > برنامه نویسی > Visual Basic 6
 چگونه نوشتن قفل با وی بی

Post Reply

1 2 3 > Last »

saeedsmk

مدیر بازنشسته



Join Date: Sep 2003
 Posts: 1,523

چگونه نوشتن قفل با وی بی

اقا می خوام به بحث شروع کنم در مورد چگونه قفل گذاشتن رو برنامه ها .
 نمی دونم این رو باید اینجا بگم و یا مثل یکی از دوستان این اطلاعات به فوته. بهر حال من که نه برنامه نویسم(حرفه ای) و نه قفل گذار پس بی خیالش 😊
 حالا هر کی نظری داره بگه که ایا باید اینجا باشه و یا تو قسمت عمومی و ...

اولین پروژه هم در مورد قفل گذاری رو فایل کامپایل شده است. سعی می کنم همه چیز رو خیلی ساده توضیح بدم (ممکنه اطلاعات من غلط باشه پس بهم بگین) اما ممکنه سخت بنظر بیاد پس پیشنهاد میکنم اسمبلی رو و چگونه ساختار فایل اجرایی رو تا حدودی بلد باشین
 این قفل رو با وی بی و اسمبلی می نویسیم . درسته وی بی در این زمینه مشکل داره ولی بهر حال کمک می کنه که شما!!!! این ضعفها رو ببندین و در نتیجه قدرت کاری شما افزایش پیدا کنه.

راستی بگم من عددی نیستم ها 😊

بامید موفقیت برای شما 😊

در دنیایی که مرگ شکارچی آن است باید شکارچی بود.
 the movie 300

..Last edited by saeedsmk; 06-20-2005 at 12:54 PM



saeedsmk

مدیر بازنشسته



Join Date: Sep 2003
 Posts: 1,523

قسمت 1

ایا شما با برنامه tzcoppy کار کردید یا نه. یه برنامه است برای تغییر iso و سپس قرار دادن یه لودر برای فایل exe که اگه فایل قفل با سایز مشخص رو سی دی نبود اون فایل اجرایی اجرا نشه و....
 این برنامه رو با وی بی نوشتن چون به runtime dll msvb نیازمنده.
 پرتکتور این برنامه میاد یه فایل exe درست میکنه و بعد از فایل شما رو به پسوند dat ذخیره کرده و....
 ولی این کار یه باگ داره اونم اینه که اگه یکی بیاد و فایل با پسوند dat رو تغییر پسوند به exe بده فایل اجرا میشه 😊
 حالا ما میخوایم همچین کاری رو بکنیم ولی یه زره پیشرفته تر یعنی اگه حتی فایل dat رو به exe تغییر داد اجرا نشه یعنی در کل فایل exe مون رو پچ نیم و یه پچر براش بنویسیم
 برای اجرا یه برنامه توسط وی بی فرمانی هست به نام shell که فایل رو اجرا کرده و بعد از اجرا فایل بر اساس تنظیمات ما سکان کشتی رو یا در اختیار فایل میرازه و یا یه برنامه ما .
 یه راه حل دیگه استفاده از api ویندوز :

:Code

```
Declare Function ShellExecute Lib "shell32.dll" Alias
"ShellExecuteA" (ByVal hwnd As Long, ByVal lpOperation As String, ByVal
lpFile As String, ByVal lpParameters As String, ByVal lpDirectory As
String, ByVal nShowCmd As Long) As Long
ویا
Declare Function ShellExecuteEx Lib "shell32.dll" Alias
"ShellExecuteEx" (SEI As SHELLEXECUTEINFO) As Long
```

خوب برای اینکه بتونیم اختیار کامل رو در دست بگیریم باید ببینیم این تابع چی کار میکنه با اصلا چه جوری یه فایل اجرایی اجرا میشه.

1-اول از همه لودر ویندوز میاد چک میکنه که ایا هدر فایل اگره درست یا نه اگه نه که به خطا گزارش میکنه
 2-اگه فایل dll داشت (که اگه تحت ویندوز باشه صد در صد داره) مبینه که چه dll رو باید استفاده کنه که این اطلاعات هم باز توی هدر فایل اگره است .

3-بعد از اون تمامی توابع api رو بر اساس نوع فایل اگره مشخص و ادرس دهی میکنه

4-بعد میاد تمامی سکشنها رو براساس این هدر توی حافظه لود میکنه (وتمامی ریسورسها رو)

5-سکشن اجرایی رو براساس خصوصیات اون سکشن با خاصیت WRC لود کرده و تمامی کالها به api رو مقدار دهی میکنه

6-بعد از اون تمامی Call های برنامه رو اگه دینامیک بود متغیر دهی کرده و کد رو آماده اجرا میکنه

8-EPO رو براساس هدر معین کرده و سپس میاد نوع اجرا رو معین کرده

9-حالا با ست کردن رجیستر esp,ebx,eds,EPI, اختیار برنامه اجرایی رو بدستش میده

این EPO =Entry point با نقطه شروع کد.که ما باهانش کار داریم(ممکنه یه لودر کارهای دیگه ای هم بکنه ولی تا اونجا که یادم بود سعی کردم همه چیز رو بنویسم و ممکنه توی ترتیب مراحل وسطی اشتباه کرده باشم ولی مهم فهم چگونه اجراست ولی مرحله 9 همیشه اخر همه هست)

بر اساس این اطلاعات میشه دید که اگه یه لودر بگیم (دستور بدیم) مرحله 9 رو اجرا نکن چی میشه هیچی فایل اجرایی ما اجرا نمیشه و به حالت معلق در میاد (suspended) و ما حالا می تونیم چک کنیم و

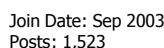
ادامه دارد 😊

..Last edited by saeedsmk; 06-25-2005 at 09:16 PM



saeedsmk

قسمت 2



:Code

E9XXXXXXXXXX

:Code

EBFE9090C0

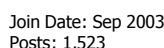
تغییر می‌دیم
خوب EB یعنی پرش از نوع نزدیک حداکثر مقدار پرش 128 تا جلو یا 127 تا عقب
عدد بعدی یعنی : مقدار ثابتی که باید بره (از بابت بعدی) رو معین می‌کنه در این حالت خاص چون عدد ما بیشتر از 128 پس پرش ما منفی شده یعنی برگشت به عقب که اینطوری حساب میشه:
مقدار کنونی(0) منهای مقداری که باید بره یعنی 2 تا عقب (برگرده به اول دستور خودش) میشه FE (هر پرش نزدیک دو بابت میگیره یکبار دستور و مقدار پرش)
بعد 90 که یعنی nop یعنی هیچ کاری نکن و بگذر (no oprate)
بعدش دوباره 90
و بعدش C0 یعنی Ret خروج از برنامه (چون هیچ الوایت نشده پس احتیاج به استفاده کردن از تابع Exitprocess و از این دست توابع نداریم)
خوب اگه کسی این برنامه رو که ما تغییر دادیم اجرا کنه چی میشه :
هیچی یا ویندوزش هنگ میکنه (خیلی خیلی کند میشه) و برنامه تو حافظه میمونه (رجیستر میشه) و باید به جوری از حافظه اونرو پاک کنه
و یا اینکه از برنامه خارج میشه (یعنی به طریقی به کد C0 میرسه).
نکته برای اطمینان بیشتر میشه کدهای بیشتری رو برداشت یعنی منظوری از ابتدا که هاست که درون برنامه قرار داره (برنامه ای که می خوایم روش قفل بگذاریم) و در نتیجه به ذره کاره رو بیشتر میشه و میشه حفاظت رو بیشتر کرد. (بعدا بیشتر توضیح می دم 😊)

..Last edited by saeedsmk; 06-27-2005 at 04:24 PM



saeedsmk

مدیر بازنشسته

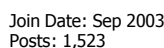


هیچکس نظری نداره؟؟؟؟؟



saeedsmk

مدیر بازنشسته



انگار کسی ایده نداره . خوب برای اینکه که کاری که شروع شده رو تموم کنیم این قسمت و فکر کنیم آخرین قسمت) در این بحث(رو میزارم .
 خوب برای مثال ما به برنامه واقعی مثل Notepad.exe رو قفل می کنیم . (وزن این برنامه 5.1.2600.2180 متعلق به ویندوز xp)
 برای این کار فایل notepad.exe رو توی به فولدر مثل work کپی میکنیم حالا با به برنامه که اطلاعات هدر فایل exe رو نشون میده برنامه notepad رو مورد
 بررسی قرار میدیم (مثل برنامه ProcDump32 توی قسمت PE Editor)
 * نکته تمامی عددها در مبنای hex می باشد

Entry Point : 739d
Size of image:14000
Image Base: 01000000

$$EP=01000000+739d=0100739d$$

:Code

```
.text
Virtual Size:00007748 مقدار فضایی که این سکشن در حافظه میگیره
Virtual Offset:00001000 ( Image base (بعلاوه
RAW Size:00007748 مقدار فضایی که این سکشن در روی هارد میگیره
Raw Offset:00000600 محل شروع در روی هارد
Characteristics:60000020 خصوصیت این سکشن مثل خواندن و نوشتن و ...
.data
Virtual Size:00001BA8 مقدار فضایی که این سکشن در حافظه میگیره
....
.rsrc
```

یعنی EP ما در حافظه برابر است با
و در قسمت سکشنها داریم: