PersianTools

?Remember Me User Name User Name
ورود Password

saeedsmk
مدير بازنشسته

Join Date: Sep 2003
Posts: 1,523

چگونگي نوشتن قفل با وي بي

اقا مي خوام يه بحث شروع كنم در مورد چگونگي قفل گذاشتن رو برنامه ها .
نمي دونم اين رو بايد اينجا بگم و يا مثل يكي از دوستان اين اطلاعات يه فوته. بهر حال من كه نه برنامه نويسم(حرفه اي) و نه قفل گذار پس بي خيالش
حالا هر كي نظري داره بگه كه ايا بايد اينجا باشه و يا تو قسمت عمومي و ...

اولين پروژه هم در مورد قفل گذاري رو فايل كامپايل شده است .سعي مي كنم همه چيز رو خيلي ساده توضيح بدم (ممكنه اطلاعات من غلط باشه پس بهم بگين) اما ممكنه سخت بنظر بياد پس پيشنهاد ميكنم اسمبلي رو و چگونگي ساختار فايل اجرايي رو تا حدودي بلد باشين
اين قفل رو با وي بي و اسمبلي مي نويسيم . درسته وي بي در اين زمينه مشكل داره ولي بهر حال كمك مي كنه كه شما!!!! اين ضعفها رو ببندين ودر نتيجه قدرت كاري شما افزايش پيدا كنه.

راستي بگم من عددي نيستم ها
باميد موفقيت براي شما

در دنيايي كه مرگ شكارچي آن است بايد شكارچي بود.
the movie 300

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

Quote

saeedsmk
مدير بازنشسته

Join Date: Sep 2003
Posts: 1,523

قسمت 1

ايا شما با برنامه tzcopy كار كرديد يا نه. يه برنامه است براي تغيير iso و سپس قرار دادن يه لودر براي فايل exeكه اگه فايل قفل با سايز مشخص رو سي دي نبود اون فايل اجرايي اجرا نشه و....
اين برنامه رو با وي بي نوشتن چون به runtime dll msvb... نيازمنده.
پرتكتور اين برنامه مياد يه فايل exe درست ميكنه و بعد از فايل شما رو به پسوند .dat ذخيره كرده و.....
ولي اين كار يه باگ داره اونم اينه كه اگه يكي بياد و فايل با پسوند dat رو تغيير پسوند به exe بده فايل اجرا ميشه
حالا ما ميخواييم همچين كاري رو يكنيم ولي يه زره پيشرفته تر يعني اگه حتي فايل dat رو به exe تغيير داد اجرا نشه
يعني در كل فايل exe مون رو پچ نيم و يه پچر براش بنويسيم
براي اجرا يه برنامه توسط وي بي فرماني هست به نام shell كه فايل رو اجرا كرده و بعد از اجرا فايل بر اساس تنظيمات ما سكان كشتي رو يا در اختيار فايل ميزاره و يا به برنامه ما .
يه راه حل ديگه استفاده از api ويندوز :

: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
 ويا
Declare Function ShellExecuteEx Lib "shell32.dll" Alias
"ShellExecuteEx" (SEI As SHELLEXECUTEINFO) As Long
```

خوب براي اينكه بتونيم اختيار كامل رو در دست بگيريم بايد ببينيم اين تابع چي كار ميكنه يا اصلا چه جوري يه فايل اجرايي احرا ميشه.
1-اول از همه لودر ويندوز مياد چك ميكنه كه ايا هدر فايل اگزه درست يا نه اگه نه كه يه خطا گزارش ميكنه
2-اگه فايل dll داشت (كه اگه تحت ويندوز باشه صد در صد داره) ميبينه كه چه dll رو بايد استفاده كنه كه اين اطلاعات هم باز توي هدر فايل اگزه است .
3-بعد از اون تمامي توابع api رو بر اساس نوع فايل اگزه مشخص و ادرس دهي ميكنه
4-بعد مياد تمامي سكشنها رو براساس اين هدر توي حافظه لود ميكنه(وتمامي ريسورسها رو)
5-سكشن اجرايي رو براساس خصوصيات اون سكشن با خاصيت WRC لود كرده و تمامي كالها به api رو مقدار دهي ميكنه
6-بعد از اون تمامي Call هاي برنامه رو اگه ديناميك بود متغيير دهي كرده و كد رو اماده اجرا ميكنه
8-EPO رو براساس هدر معين كرده وسپس مياد نوع اجرا رو معين كرده
9-حالا با ست كردن ريجستر esp,ebx,eds,EPI, اختيار برنامه اجرايي رو بدستش ميده
اين EPO =Entry point يا نقطه شروع كد.كه ما باهاش كار داريم(ممكنه يه لودر كار هاي ديگه اي هم بكنه ولي تا اونجا كه يادم بود سعي كردم همه چيز رو بنويسم و ممكنه توي ترتيب مراحل وسطي اشتباه كرده باشم ولي مهم فهم چگونگي اجراست ولي مرحه 9 هميشه اخر همه هست)

بر اساس اين اطلاعات ميشه ديد كه اگه به لودر بگيم (دستور بديم) مرحله 9 رو اجرا نكن چي ميشه هيچي فايل اجرايي ما اجرا نيمشه و به حالت معلق در مياد (suspended) و ما حالا مي تونيم چك كنيم و ....

ادامه دارد

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

Quote

saeedsmk

قسمت 2

Join Date: Sep 2003
Posts: 1,523

حالا فرض كنيم كه اين اتفاق افتاد يعني اينكه برنامه معلق شد .چيكار بايد بكنيم
فرض كنيم كه نقطه شروع برنامه ما در حافظه 401000 باشه ودر افست (بيت) 0x445B كد برنامه (به هگزه) و شامل اطلاعات

:Code

```
E9XXXXXXXX
```

كه يعني به نقطه اي از حافظه بپر .
خوب ما اين كد رو با يه برنامه (يك هگزه اديتور و يا برنامه اي كه مي شه نوشت) به مقادير

:Code

```
EBFE9090C0
```

تغيير ميديم
خوب EB يعني پرش از نوع نزديك حداكثر مقدار پرش 128 تا جلو يا 127 تا عقب
عدد بعدي يعني : مقدارياتي كه بايد بپره (از بايت بعدي) رو معين مي كنه در اين حالت خاص چون عدد ما بيشتر از 128 پس پرش ما منفي شده يعني برگشت به عقب كه اينطوري حساب ميشه:
مقدار كنوني(0) منهاي مقداري كه بايد بپره يعني 2 تا عقب (برگرده به اول دستور خودش) ميشه FE (هر پرش نزديك دو بايت ميگيره يكي دستور EB و مقدار پرش)
بعد 90 كه يعني nop يعني هيچ كاري نكن و بگذر (no oprate)
بعدش دوباره 90
و بعدش C0 يعني Ret خروج از برنامه (چون هيچ الوكيت نشده پس احتياج به استفاده كردن از تابع Exitprocess و از اين دست توابع نداريم)
خوب اگه كسي اين برنامه رو كه ما تغيير داديم اجرا كنه چي ميشه :
هيچي يا ويندوزش هنگ ميكونه (خيلي خيلي كند ميشه) و برنامه تو حافظه ميمونه (رجيستر ميشه) و بايد يه جوري از حافظه اونرو پاك كنه و يا اينكه از برنامه خارج ميشه (يعني به طريقي به كد C0 ميرسه).
نكته براي اطمينان بيشتر ميشه كدهاي بيشتري رو برداشت يعني منظورم از ابتدا كد هاست كه درون برنامه قرار داره (برنامه اي كه مي خوايم روش قفل بگذاريم) و در نتيجه يه ذره كار ها بيشتر ميشه و ميشه حفاظت رو بيشتر كرد .(بعدا بيشتر توضيح مي دم)

حالا ما بايد به عنوان برنامه نويس يه لودربراي اين برنامه تحت ويندوز بسازيم و بعد از لود كامل فايل اجراي اون رو تغيير بديم و به كد اصلي برگردونيم تا برنامه درست عمل كنه مثل يه پكر

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

Quote

---

saeedsmk
مدير بازنشسته

Join Date: Sep 2003
Posts: 1,523

هيچكس نظري نداره؟؟؟