بسمه تعالی

اول : نکته کنکوری : من چون کامپیوترم آلوده نبود ، صحت کارکرد این آنتی ویروس را نتونستم چک کنم .
نکته دوم غیر کنکوری : این آموزش رایگان است .

اول فایل **ollydbg** را که یک دیباگر حافظه هست را اجرا کنید
از منوی **Open– File**
فایل **MagicRecover.exe** را انتخاب کنید (این فایل مثلا یک آنتی ویروس خارجی هست به آدرس : **http://magicrecover.clanteam.com**
با قیمت 39 دلار ولی این آدرس چند روزی بیشتر نیست که ساخته شده (توی گوگل تا این لحظه که ایندکس نشده)
حتی از روی عجله یادش رفته اطلاعات دسترسی به **FTP** را هم مواظب باشه **J**
USER magicrecover_clanteam
PASS clanteam_com
نکته کنکوری : احمقها کم نیستند. این خره هم یکی از اونهاست که پول درآوردن به هر قیمتی براش مهم نیست!(شاید بعد از این مطلب اقدام به تعویض پسورد بکنه ولی دیگه مهم نیست چون اول فایل اصلی ضمیمه این آموزش هست ، دوم برای حذف محدودیت **demo** نیازی به اینترنت اصلا نیست)
خب چی میگفتم ؟ آهان..
Shift+F9 را یک یا چندبار بزنید تا منوی اول برنامه بیاد
در این حالت به برنامه **ollydbg** برگردید و کلید **Ctrl+G** را بزنید و در منوی آن تایپ کنید:
0042A7BF
خب برنامه میپره به یک نقطه ای که با این مقدار برابر هست ، بدون اینکه به چیزی دست بزنید کلید **F2** را بزنید (باید قرمز رنگ بشه)
خب **olly** را مینیمایز کنید و کلید **Demo** را از برنامه بزنید
خب به برنامه **olly**برگردید میبینید طبق شکل زیر یک مقداری را میبینید ، مثلا برای کامپیوتر من **28377.66** نوشته شده (این عدد بر اساس سریال هارد دیسک شما بدست میاد و برای هر کامپیوتری منحصر به فرد هست ، در حالت معمولی باید وصل بشین اینترنت و فقط 5تافایل را بازیابی میکنه)
! (گاهی وقتها آدم دلش میخواد فحشش بده **J**) خودتون هرچی دوست داشتین حواله اش کنید ....

OllyDbg - MagicRecover.exe - [CPU - main thread, module MagicRec]

File View Debug Options Window Help

```
0042A7BF  . 50              PUSH EAX
0042A7C0  . FF15 58104000   CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrC  MSVBVM60.__vbaStrCat
0042A7C6  . 8BD0            MOV EDX,EAX
0042A7C8  . 8D4D C8         LEA ECX,DWORD PTR SS:[EBP-38]
0042A7CB  . FF15 F4114000   CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrM  MSVBVM60.__vbaStrMove
0042A7D1  . 50              PUSH EAX
0042A7D2  . 68 EC844000     PUSH MagicRec.004084EC                  UNICODE ".txt"
0042A7D7  . FF15 58104000   CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrC  MSVBVM60.__vbaStrCat
0042A7DD  . 8BD0            MOV EDX,EAX
0042A7DF  . 8D4D D0         LEA ECX,DWORD PTR SS:[EBP-30]
0042A7E2  . FF15 F4114000   CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrM  MSVBVM60.__vbaStrMove
0042A7E8  . 8D4D C8         LEA ECX,DWORD PTR SS:[EBP-38]
0042A7EB  . FF15 2C124000   CALL DWORD PTR DS:[<&MSVBVM60.__vbaFree  MSVBVM60.__vbaFreeStr
0042A7F1  . C745 FC 11000   MOV DWORD PTR SS:[EBP-4],11
0042A7F8  . 8D4D D0         LEA ECX,DWORD PTR SS:[EBP-30]
0042A7FB  . 898D 38FFFFFF   MOV DWORD PTR SS:[EBP-C8],ECX
0042A801  . C785 30FFFFFF   MOV DWORD PTR SS:[EBP-D0],4008
0042A80B  . 8D95 30FFFFFF   LEA EDX,DWORD PTR SS:[EBP-D0]
0042A811  . 52              PUSH EDX
0042A812  . FF15 D8104000   CALL DWORD PTR DS:[<&MSVBVM60.#529>]    MSVBVM60.rtcKillFiles
0042A818  . C745 FC 12000   MOV DWORD PTR SS:[EBP-4],12
0042A81F  . C785 38FFFFFF   MOV DWORD PTR SS:[EBP-C8],MagicRec.0040  UNICODE "ftp://magicrecover.clanteam.com"
0042A829  . C785 30FFFFFF   MOV DWORD PTR SS:[EBP-D0],8
0042A833  . B8 10000000     MOV EAX,10
0042A838  . E8 7384FDFF     CALL <JMP.&MSVBVM60.__vbaChkstk>
0042A83D  . 8BC4            MOV EAX,ESP
0042A83F  . 8B8D 30FFFFFF   MOV ECX,DWORD PTR SS:[EBP-D0]
0042A845  . 8908            MOV DWORD PTR DS:[EAX],ECX
0042A847  . 8B95 34FFFFFF   MOV EDX,DWORD PTR SS:[EBP-CC]
0042A84D  . 8950 04         MOV DWORD PTR DS:[EAX+4],EDX
0042A850  . 8B8D 38FFFFFF   MOV ECX,DWORD PTR SS:[EBP-C8]
0042A856  . 8948 08         MOV DWORD PTR DS:[EAX+8],ECX
0042A859  . 8B95 3CFFFFFF   MOV EDX,DWORD PTR SS:[EBP-C4]
0042A85F  . 8950 0C         MOV DWORD PTR DS:[EAX+C],EDX
0042A862  . 6A 09           PUSH 9
0042A864  . 8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
0042A867  . 8B08            MOV ECX,DWORD PTR DS:[EAX]
0042A869  . 8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
0042A86C  . 52              PUSH EDX
0042A86D  . FF91 18030000   CALL DWORD PTR DS:[ECX+318]
0042A873  . 50              PUSH EAX
0042A874  . 8D45 C0         LEA EAX,DWORD PTR SS:[EBP-40]
0042A877  . 50              PUSH EAX
```

EAX=0017BDAC, (UNICODE "28377.66")

```
Registers (FPU)
EAX 0017BDAC UNICODE "28377.66"
ECX 0015A7C8
EDX 0015FA24 UNICODE "D:\WINDOWS\s
EBX 00000001
ESP 0012F35C
EBP 0012F514
ESI 0012F5F0
EDI 0012F520

EIP 0042A7BF MagicRec.0042A7BF

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (000000

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,

ST0 empty +UNORM 1F80 00000000 000
ST1 empty +UNORM 0040 00000040 000
ST2 empty -UNORM B37C 00000000 000
ST3 empty 5.9109082616230209040e-4
ST4 empty 5.9692503306118258680e-4
ST5 empty 4.6710181118096193770e-4
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000
               3 2 1 0      E S P
FST 4000  Cond 1 0 0 0  Err 0 0 0
FCW 137F  Preo NEAR,64  Mask    1
```

```
Address   Hex dump                 ASCII
00430000  00 00 00 00 00 00 00 00  ........
00430008  30 E9 15 00 00 00 00 00  0θ§.....
00430010  20 F6 15 00 00 00 00 00   ÷§.....
00430018  00 00 00 00 30 EA 15 00  ....0Ω§.
00430020  00 00 00 00 00 00 00 00  ........
00430028  24 FA 15 00 5C F1 15 00  $·§.\±§.
00430030  C4 F1 15 00 AC BD 17 00  -±§.¼╜↨.
00430038  6C FA 15 00 00 00 00 00  l·§.....
00430040  00 00 00 00 00 00 00 00  ........
```

```
0012F35C  0015FA24  UNICODE "D:\WINDOWS\system32\
0012F360  0012F520
0012F364  0012F5F0
0012F368  00000001
0012F36C  00000000
0012F370  00000000
0012F374  00000000
0012F378  00000000
0012F37C  00000000
0012F380  00000000
0012F384  00000000
```

خب کار تقریبا تمامه :

برنامه **olly** را ببنید ، ویک **Notepad** باز کنید (به منوی **run** ویندوز بروید و در آن تایپ کنید**notepad** و اینتر بزنید ، کار سختی بود نه **J**))

خب این مقدار که پیدا کردید را در آن بنویسید و بعد به منوی **save** رفته و آن را به این اسم ذخیره کنید

D:\WINDOWS\system32\v_set.dat

توجه کنید که آدرس درایو وفولدر ویندوز شما ممکنه با مال من فرق کنه ، ولی **system32\v_set.dat** آن همیشه ثابته

خب همین برنامه اجرا کنید و اجازه بدین ویروس یابی کنه و هم فایلهای خراب شده را ریکاور کنه

پیوست : به هیچ کس باج ندین ، همیشه هستند کسانی که وقت زیادی شاید بزارند، ولی اجازه ندن کسی فکر باج گرفتن به سرش بزنه.

(کلاس و هندونه برای خودم)

پیوست 2: همیشه ویروسها در شکلها و نوع های مختلف هر روزه به وسیله عده ای بی وجدان تولید میشوند ، آنتی ویروسها همیشه نمیتوانند یک ویروس که صبح همون روز یکی از این بی وجدانها نوشته را شناسائی کنند ، پس غیر از داشتن آنتی ویروس اطلاعات عمومی خود را نسبت به کامپیوتر ، روشهای الوده شدن به ویروسها و غیره به روز کنید ، در اینترنت انجمنهای فارسی آموزشی زیادی پیدا میشوند مثلا همین انجمن خودمون که این بحث در اون مطرح شد ، **http://www.iranled.com/forum**

پیوست 3: همیشه روشهای عمومی (یونیورسال) برای جلوگیری از آلوده شدن به وسیله ویروسها هست. پس سعی کنید یک قدم از آنتی ویروسها و ویروسها جلوتر باشید. (سوال بپرسید ، تجربه کسب کنید ، توی سر و مغز کامپیوتر بزنید ، حتی مثل ما شبها بیخوابی بکشید ولی یاد بگیرید که یهو یک روز صبح پا نشین ببینین یه ویروس فزرتی همه شغل و آبرو و زندگیتون را یک شبه به باد داده) علاج واقعه قبل از حادثه !(ضرب المثل ورژن جدید)

تشکر پیوست : از امین تاتو با آیدی جدیدش **Mr.programmer** در سایت **iranLed** هم بابت اطلاع رسانی برای شناسائی ویروس در اختیار دادن لینک دانلود این آنتی ویروس خارجی !!!!! تشکر ویژه میکنیم.

Joker

www.Shabgard.org **www.IranLed.com**