

Pandora'nın Kutusu Nasıl Açılır ?

written by Mert SARICA | 5 August 2010

Zararlı yazılım analistini nedense meraklı Pandora'ya benzetirim çünkü işi gereği kötülük ile dolu olan o kutuyu (paketlenmiş zararlı yazılım) açarak kötülüğün tüm işletim sistemine hakim olmasına neden olur fakat efsanenin aksine kutuyu kapatmaya çalışmaz çünkü analistin tek amacı zararlı yazılımı baştan sona analiz edebilmektir.

Daha önceki yazılarımda da belirttiğim üzere art niyetli kişiler zararlı yazılımların disk üzerinde antivirüs ve benzer koruma yazılımları tarafından tespit edilmesini ve ayrıca zararlı yazılımın analiz edilmesini zorlaştırma adına paketleyici (packer) yazılımlar kullanırlar. Fakat bilinenin aksine bu yazılımların asıl kullanım amacı hedef programın diskte kapladığı yeri azaltmaktır çünkü bu yazılımlar ile paketlenen programların boyutunun yarı yarıya azaldığı bilinmektedir.

Hem iyi hemde art niyetli kişiler arasında en çok tercih edilen paketleme yazılımlarının başında UPX gelir. Art niyetli kişiler arasında tercih edilmesinin en büyük nedenleri arasında ücretsiz olması ve çoğu zararlı kod paketleyici yazılımının UPX yazılımını içeriyor olmasıdır.

UPX veya herhangi bir paketleyici yazılım ile paketlenmiş bir programın analiz edilebilmesi için öncelikle paket içinden çıkartılması gerekmektedir. Örnek olarak UPX ile paketlenmiş bir programı ele alacak olursak bu programı analiz edebilmek için yapılması gereken ilk iş ya debugger (ollydbg) ile çalıştırmak yada paket açma işini otomatik olarak gerçekleştiren araçlardan faydalanmak olacaktır fakat bu araçlar paketleme yazılımların yeni sürümlerinin yayınlanmasından sonra beklentileri karşılayamadıkları için çoğu zaman debugger ile çalıştırmak ve analiz etmek gerekmektedir fakat ben iki yoldan da kısaca bahsedeceğim.

Örnek olarak UPX ile calc.exe (windows hesap makinası) programını sıkıştırdığımızda programın boyutunun %49 oranında ufaldığını görüyoruz.

```

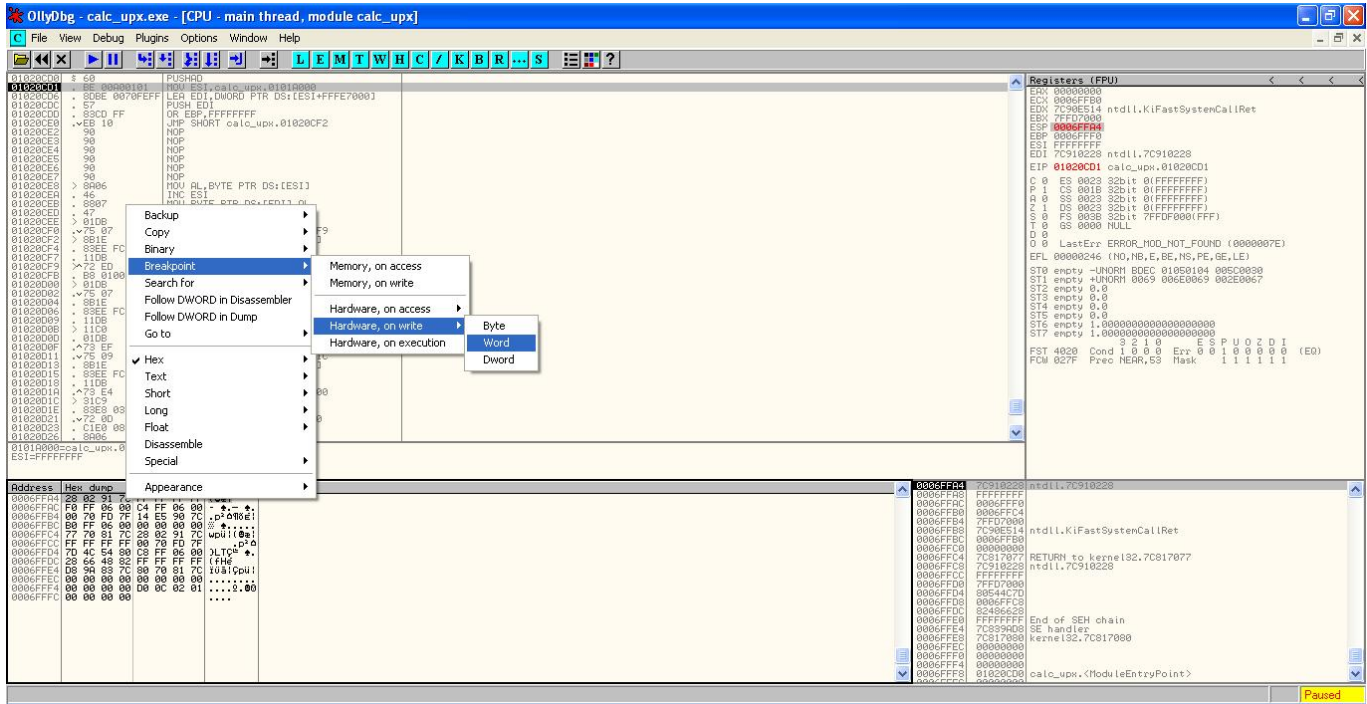
C:\Documents and Settings\Administrator\Desktop>upx calc.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2010
UPX 3.05w Markus Oberhumer, Laszlo Molnar & John Reiser Apr 27th 2010

File size   Ratio   Format   Name
-----
114688 -> 56832 49.55%  win32/pe  calc.exe

Packed 1 file.

```

calc_upx.exe programını Ollydbg ile açtığımız zaman normal programlarda karşılaştığımız fonksiyon prologue'nin aksine PUSHAD ile karşılaşırız. PUSHAD tüm register değerlerini stack'e kopyalamaya yaramaktadır ve UPX ve ASPack gibi paketleme yazılımlarında PUSHAD sonrasında paketlenmiş veri açılır ve daha sonrasında POPAD ile daha önce stack'e kaydedilmiş olan değerler register'a geri kopyalanır. Paketlenmiş programlarda EP (entry point) paketin açılmasını sağlayan fonksiyonu işaret eder ve paket açıldıktan sonra OEP (original entry point) sayesinde program çalışabilmesi için ilgili bölüme (section) yönlendirilir. Amacımız OEP'ini bulmak olduğu için ve programın çalışabilmesi için öncelikle paketin açılması gerektiği ve ardından ilgili bölüme gitmesi gerektiği için OEP'in bilinmesi gerekmektedir. Bunun için PUSHAD ile saklanan ESP register'ına hardware on access breakpoint koyarsak, POPAD komutu ile eninde sonunda bu değer register'a geri kopyalanacağı için breakpoint sayesinde POPAD'e kısa yoldan gidebilir ve OEP'ini tespit edebiliriz.

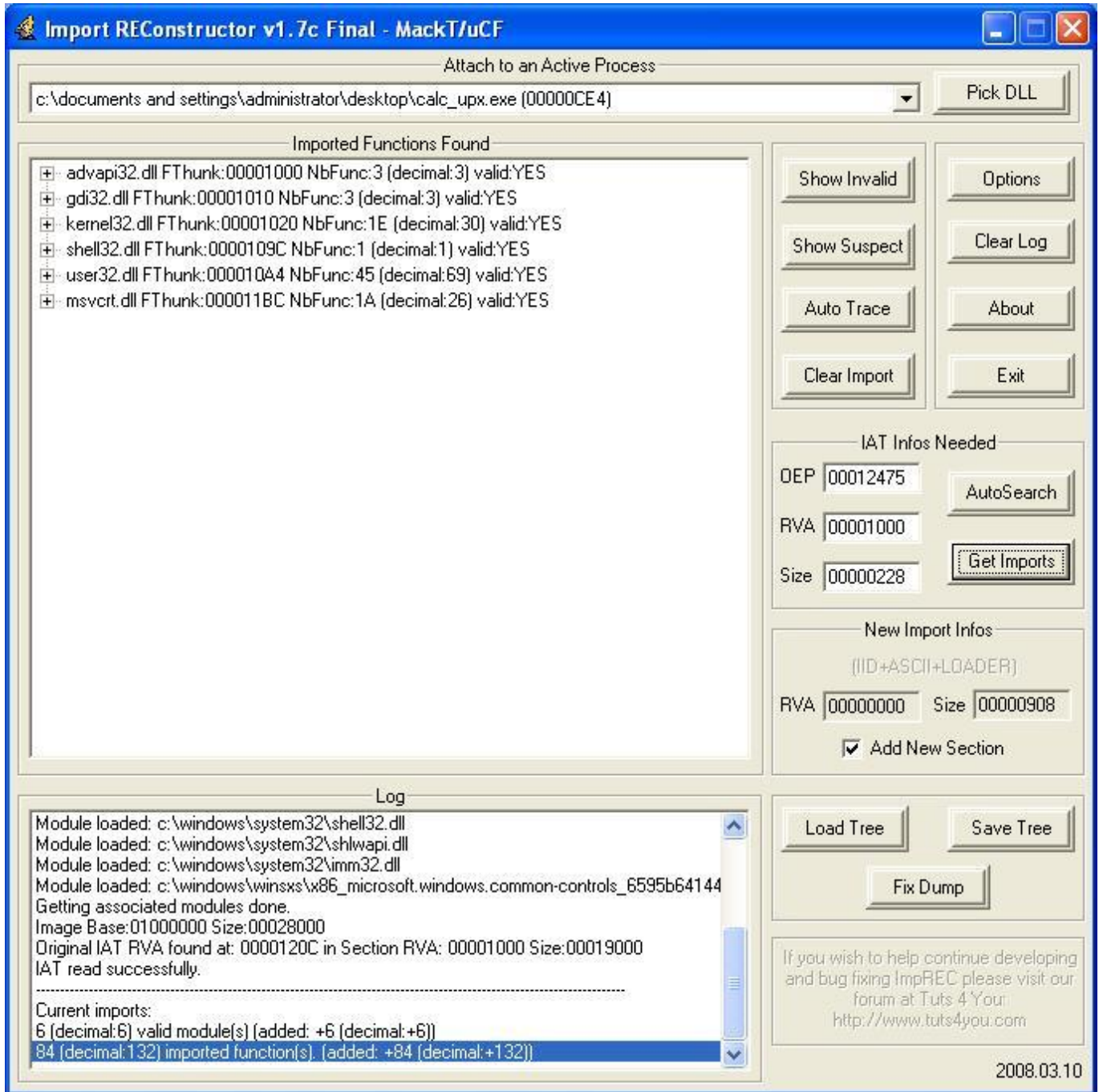


OEP'ini tespit ettikten sonra Ollydbg eklentisi olan Ollydump ile paketi açılmış olan programı (calc_upx.exe) diske kayıt (dump) edebiliriz.

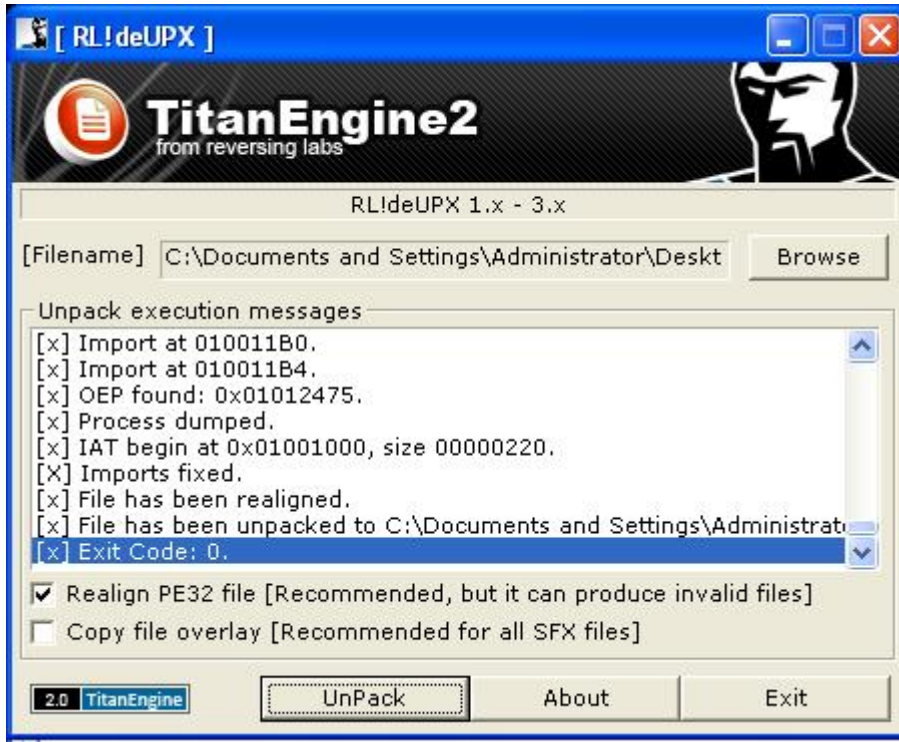
The screenshot shows the OllyDbg interface with the following components:

- Assembly View:** Displays assembly instructions for `kernel32.GetModuleHandleA`. The instruction list includes:
 - `6A 76 PUSH 76`
 - `68 E0150001 PUSH calc_upx.01001500`
 - `E8 47030000 CALL calc_upx.010127C8`
 - `33B6 XOR EBX,EBX`
 - `63 PUSH EBX`
 - `8E30 20100001 MOV EDI, DWORD PTR DS:[00101020]`
 - `FFD7 CALL EDI`
 - `66:0130 405A JMP WORD PTR DS:[ERX+5040]`
 - `75 1F JNZ SHORT calc_upx.010124B2`
 - `8B48 3C MOV ECX, DWORD PTR DS:[ERX+3C]`
 - `83C8 XOR ECX,ECX`
 - `8139 50450000 CMP DWORD PTR DS:[ECX], 4550`
 - `75 12 JNZ SHORT calc_upx.010124B2`
 - `8F67 18 JNZ WORD PTR DS:[ECX+18]`
 - `30 00910000 JMP EBX,100`
 - `74 1F JEC SHORT calc_upx.010124C4`
 - `30 00020000 JMP EBX,200`
 - `74 0E JEC SHORT calc_upx.010124B7`
 - `895D E4 MOV DWORD PTR SS:[EBP-1C],EBX`
 - `75 27 JNZ SHORT calc_upx.010124D6`
 - `8369 04000000 0 CMP DWORD PTR DS:[ECX+84],0E`
 - `76 F2 JBE SHORT calc_upx.010124B2`
 - `33C0 XOR EBX,EBX`
 - `3999 F8000000 CMP DWORD PTR DS:[ECX+FA],EBX`
 - `75 0E JNZ SHORT calc_upx.010124D8`
 - `76 E2 JBE SHORT calc_upx.010124B2`
 - `33C0 XOR EBX,EBX`
 - `3999 E8000000 CMP DWORD PTR DS:[ECX+EA],EBX`
 - `8F9E0B SETNE AL`
 - `8945 E4 MOV DWORD PTR SS:[EBP-1C],EBX`
 - `895D FC MOV DWORD PTR SS:[EBP-4],EBX`
 - `6A 02 PUSH 2`
 - `FF15 0C120001 CALL DWORD PTR DS:[100120C1]`
 - `68 49 POP ECX`
 - `8380 10500101 0 FOR DWORD PTR DS:[10150101],FFFFFFFF`
 - `8380 14500101 0 FOR DWORD PTR DS:[10150101],FFFFFFFF`
 - `FF15 0C120001 CALL DWORD PTR DS:[100120C1]`
 - `8B00 0C500101 MOV ECX, DWORD PTR DS:[101500C]`
 - `8988 MOV DWORD PTR DS:[ERX],ECX`
 - `FF15 04120001 CALL DWORD PTR DS:[10012041]`
- Registers (FPU):** Shows register values such as `EAX: 00000144`, `ECX: 0006FFB0`, `EDX: 7C910228`, `EIP: 01012475`.
- OllyDump Dialog:** A window titled "OllyDump - calc_upx.exe" is open, showing:
 - Start Address: 1000000, Size: 28000
 - Entry Point: 20C0D, Modify: 12475, Get EIP as OEP
 - Base of Code: 1A000, Base of Data: 21000
 - Options: Fix Raw Size & Offset of Dump Image
 - Table with columns: Section, Virtual Size, Virtual Offset, Raw Size, Raw Offset, Characteristics.
 - Method selection: Method1: Search JMP/JAPI | CALL/JAPI in memory image
- Memory Dump:** Shows hex and ASCII data for addresses from `000FFFA4` to `000FFFC4`.

Diske kayıt edilmesiyle Import adres tablosu (import edilen modüller ve fonksiyonlar) bozulan programı analiz edebilmek ve tekrar çalıştırabilmemiz için impREC programı ile import tablosunu düzelttikten sonra amacımıza ulaşmış oluruz.



Tabiiki UPX veya benzer yazılımlar ile paketlenen programları paketten çıkartmak için her defasında böyle uğraşmamıza gerek yok çünkü piyasada bu yazılımlar ile paketlenmiş programları otomatik olarak çözen programlar mevcut. Örnek olarak ReversingLabs firması tarafından hazırlanmış olan deUPX programını ücretsiz olarak temin edebilirsiniz.



Programların yanı sıra internette bu işi otomatize etmek ve kendi paket açma aracınızı hazırlamak için kütüphaneler de bulabilirsiniz. Mesela Blackhat konferanslarında bol bol sunum yapan ReversingLabs firmasının geliştirdiği TitanEngine kütüphanesini duymuş olabilirsiniz. Duymadıysanız Titanengine, içinde entegre debugger, disassembler bulunduran ve yukarıda manuel olarak gerçekleştirilen işlemleri otomatik olarak gerçekleştirmenizi sağlayan ve 400 fonksiyonu kullanmanıza imkan tanıyan oldukça başarılı bir kütüphanedir. Zararlı yazılım analizi ile yakından ilgileniyorsanız bu kütüphaneye göz atmanızı şiddetle tavsiye eder, bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim.