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.

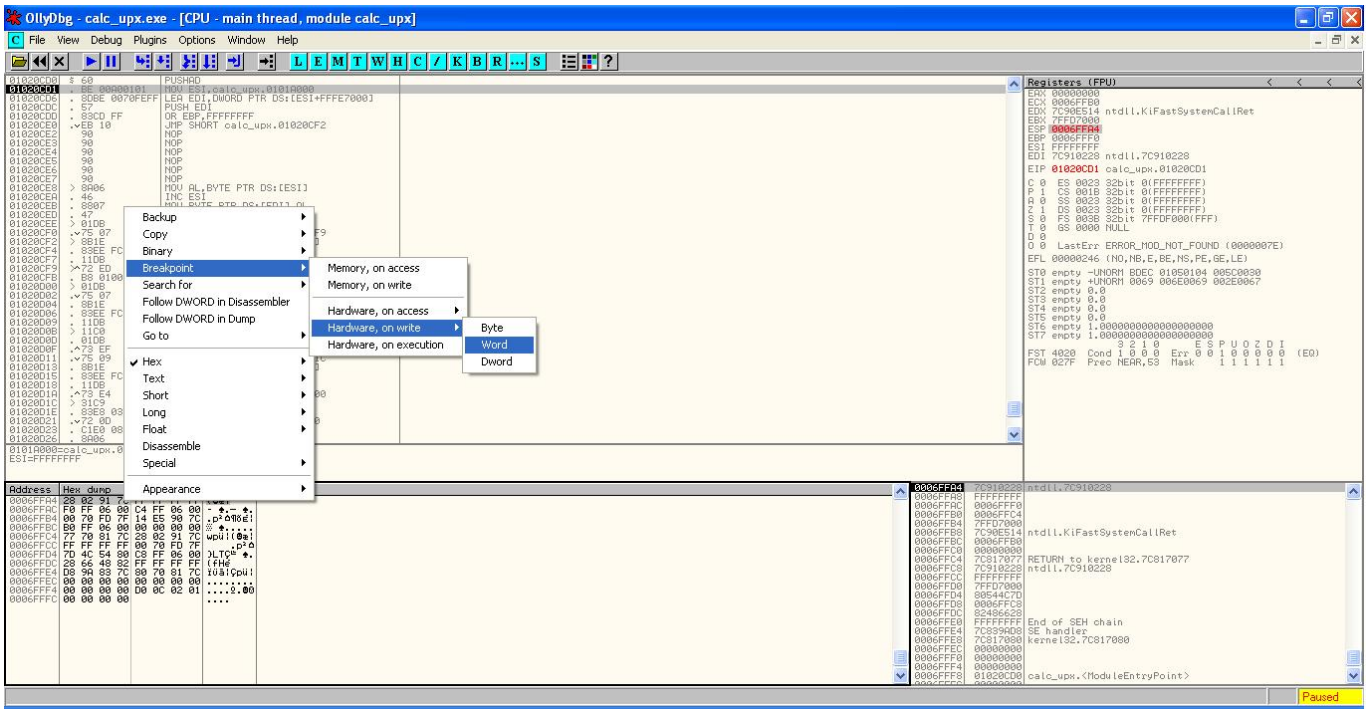
Hem iyi hemde art niyetli kişiler arasında en çok tercih edilen paketleme yazılımlarının başında UPX gelir. Art niyetli kişiler arasında tercih edilmesinin en büyük nedenleri arasında ücretsiz olması ve çoğu zararlı kod paketleyici yazılımının UPX yazılımını içeriyor olmasıdır.

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.

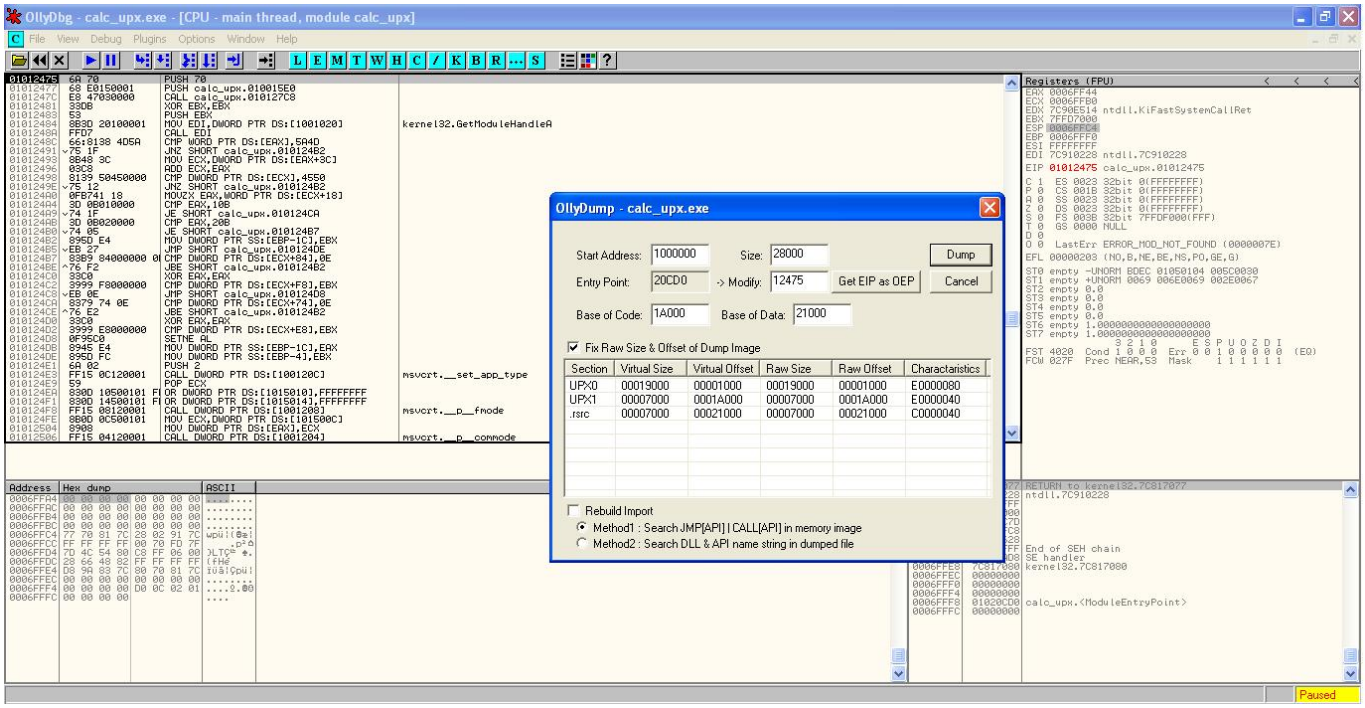
Örnek olarak UPX ile calc.exe (windows hesap makinası) programını sıkıştırdığımızda programın boyutunun %49 oranında ufaldığını görüyoruz.

```
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.
```

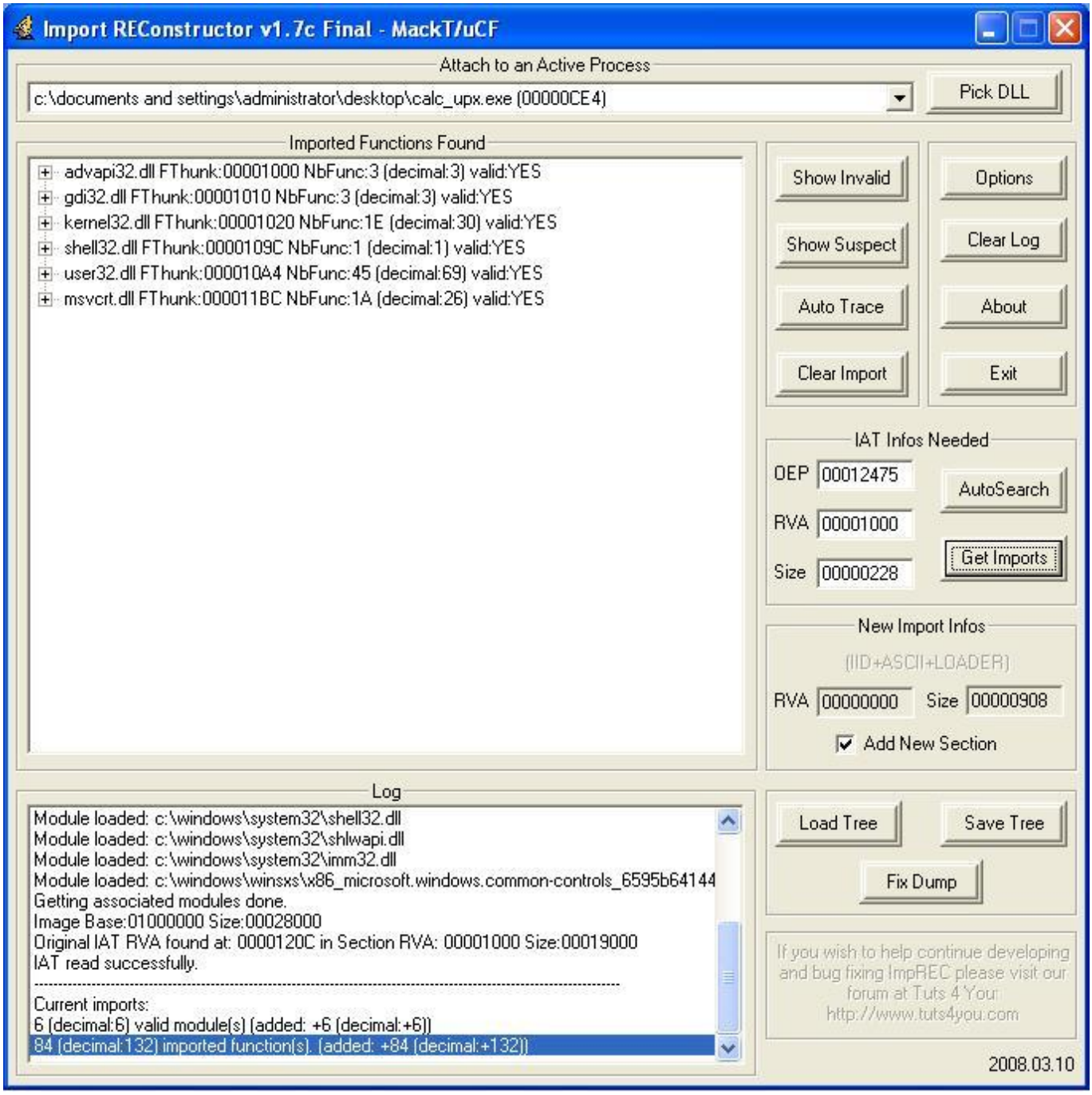
calc_upx.exe programını Ollydbg ile açtığımız zaman normal programlarda karşılaştığımız fonksiyon prologue'nin aksine PUSHAD ile karşılaşıyoruz. PUSHAD tüm register değerlerini stack'e kopyalamaya yaramaktadır ve UPX ve ASPack gibi paketleme yazılımlarında PUSHAD sonrasında paketlenmiş veri açılır ve 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'i 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 registera geri kopyalanacağı için breakpoint sayesinde POPAD'e kısa yoldan gidebilir ve OEP'i tespit edebiliriz.



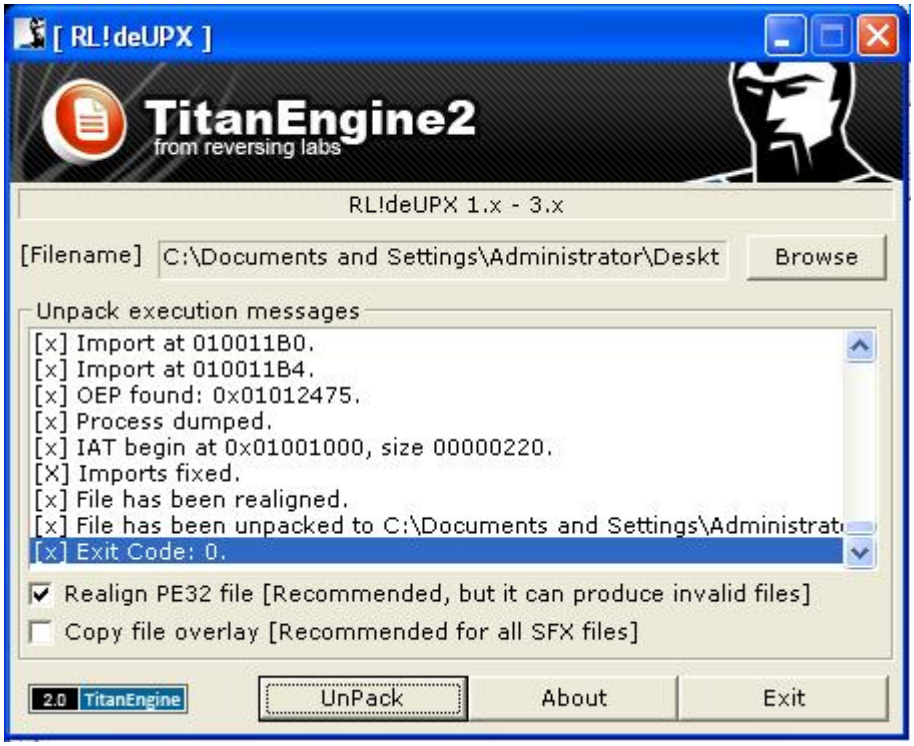
OEP'i tespit ettikten sonra Ollydbg eklentisi olan Ollydump ile paketi açılmış olan programı (calc_upx.exe) diske kayıt (dump) edebiliriz.



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 yukarda 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.