第四十五章-ReCrypt v0.80 脱壳(续)

本章是对上一章节的补充。

本章我们需要用到几款工具,分别是

1.OllyGhost(DIY 过的 OllyDbg)(PS:OllyGhost 压根没用上,在 XP 下运行会提示无法在 NT 系统运行,大家还是用原版 OD 吧)

2.OllyDump(OD 的 dump 插件)

3.LordPE

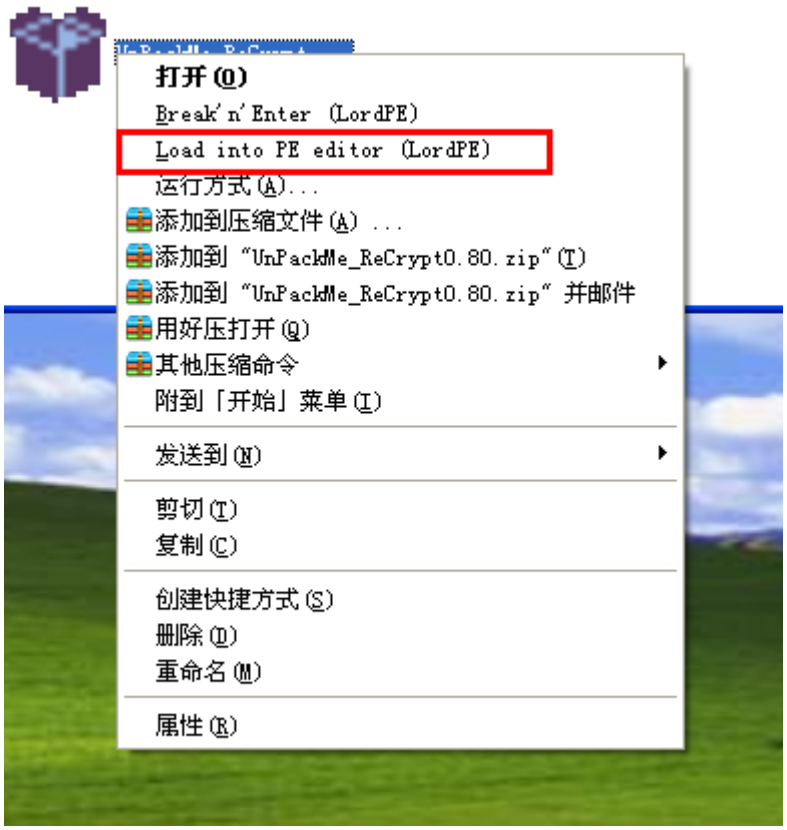
4.Estricnina_v0.12

5.POKEMON_AntiAttach

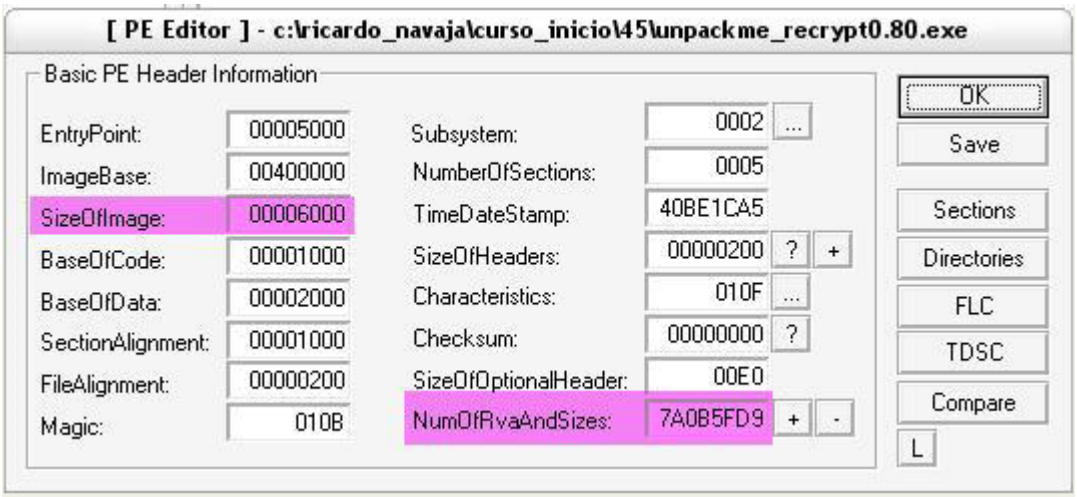
信息收集:

在我们开始分析 UnPackMe_ReCrypt0.80.exe 之前,首先用 LordPE 查看一下该程序 PE 的信息。

直接选中该程序单击鼠标右键选择 Load into PE editor(LordPE)(PS:还记得上一章节介绍过的这个系统菜单项吧)



这样我们 LordPE 的 PE 编辑器就直接打开了该程序,比较方便。



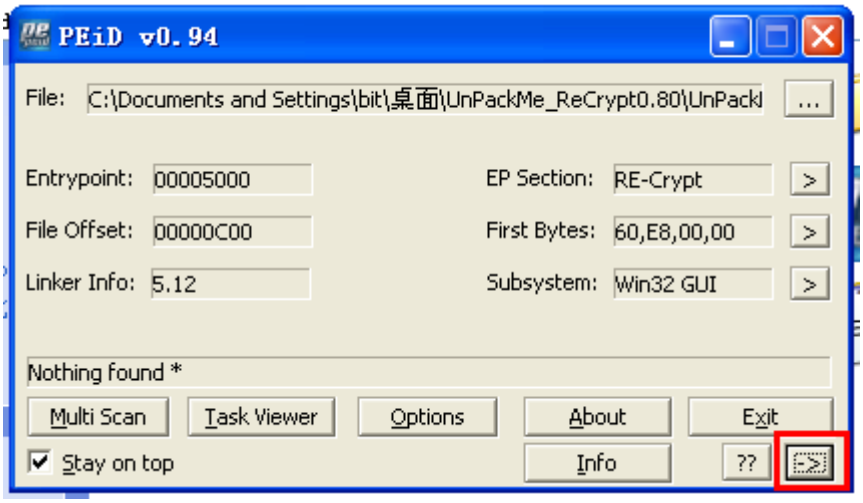
这些字段非常重要,因为很多壳在解密区段的过程中会修改这些字段。我们可以看到这里 NumOfRvaAndSizes 字段就被修改过了。

因为一般来说这个字段的值为 0x10,不可能是 0x7A0B5FD9 这么大一个值。

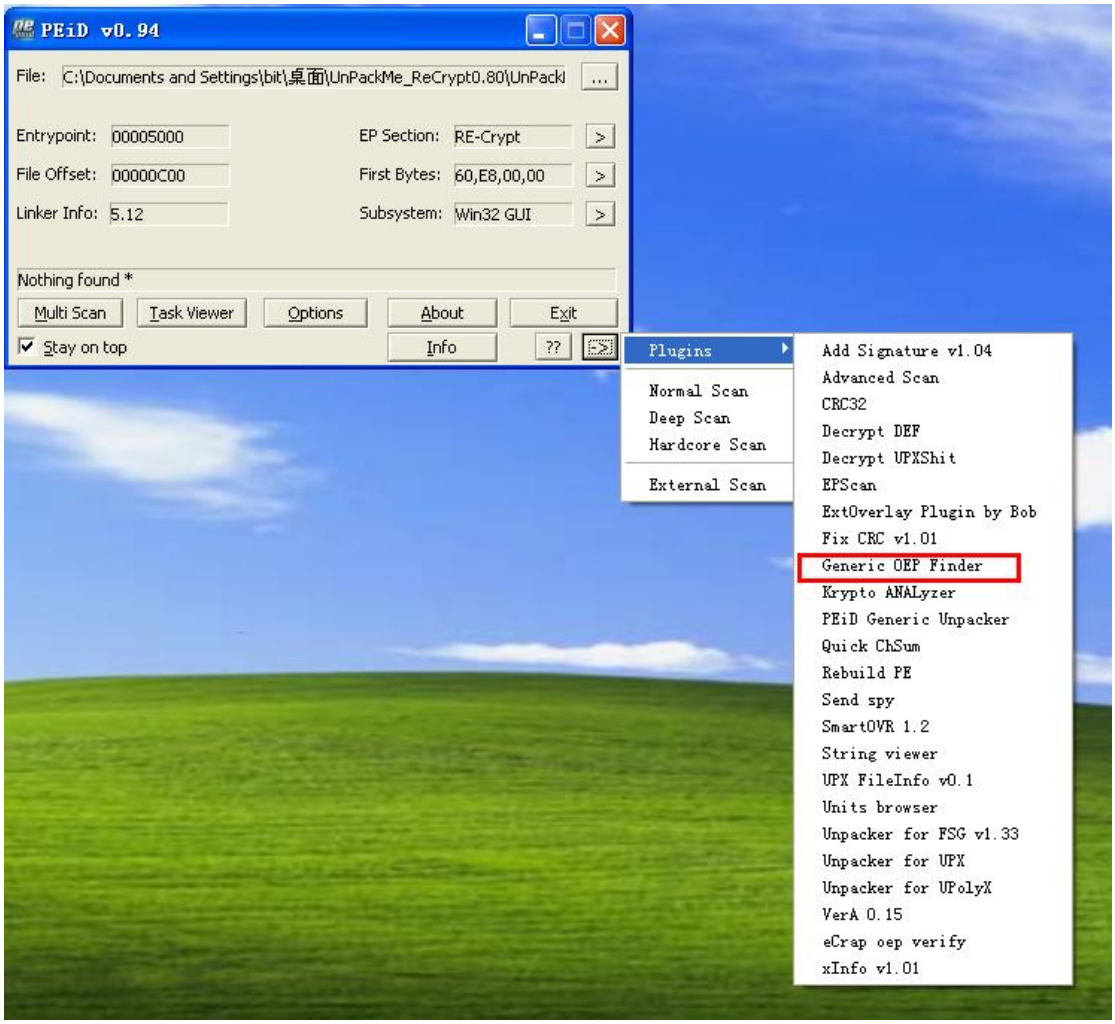
这里 NumOfRvaAndSizes 这个字段的偏移是 0xB4。

接下来我们需要定位该程序的 OEP,这里我们使用 PEID 的 Generic OEP Finder 插件来定位。

将 UnPackMe_ReCrypt0.80.exe 拖拽到 PEID 中,单击 PEID 主界面右下方的右箭头按钮。



会弹出一个菜单,我们选中 Plugins(插件)菜单,接着选中 Generic OEP Finder 菜单项。



不一会儿就会弹出一个消息框,显示 OEP 为 0x401000。

好了,信息已经搜集完毕了。下面我们来展开攻击。

收集到的信息如下:

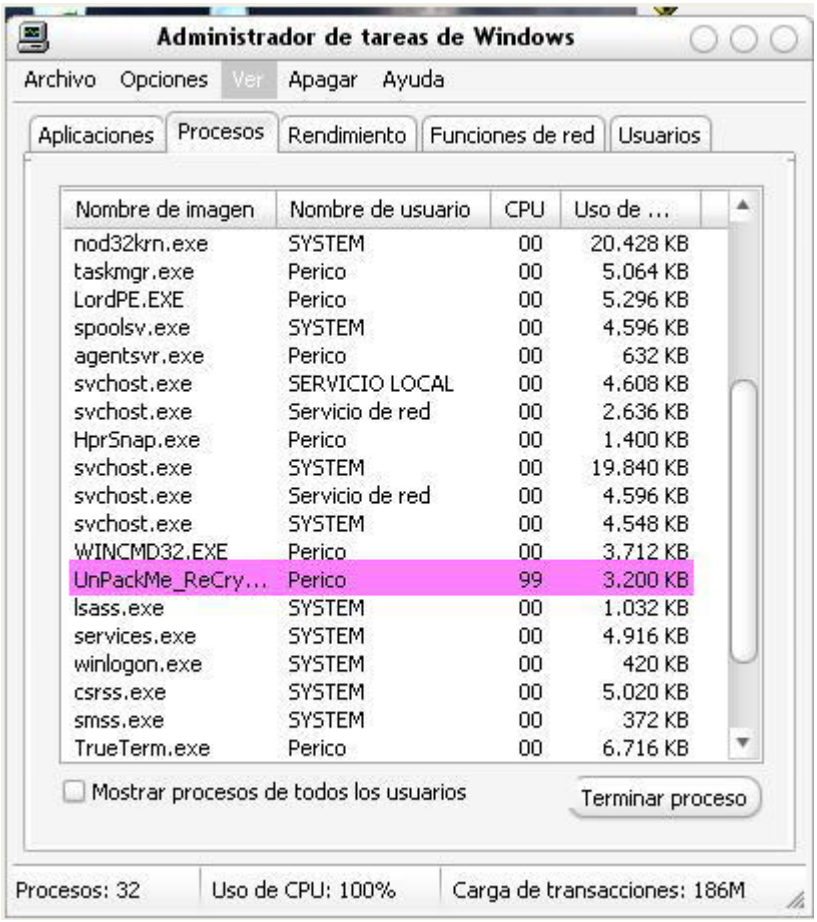
1.OEP　00401000

2.SizeOfImage 00006000

3.NumberOfRvaAndSizes 偏移 0xB4, 我们修改为了 0x10

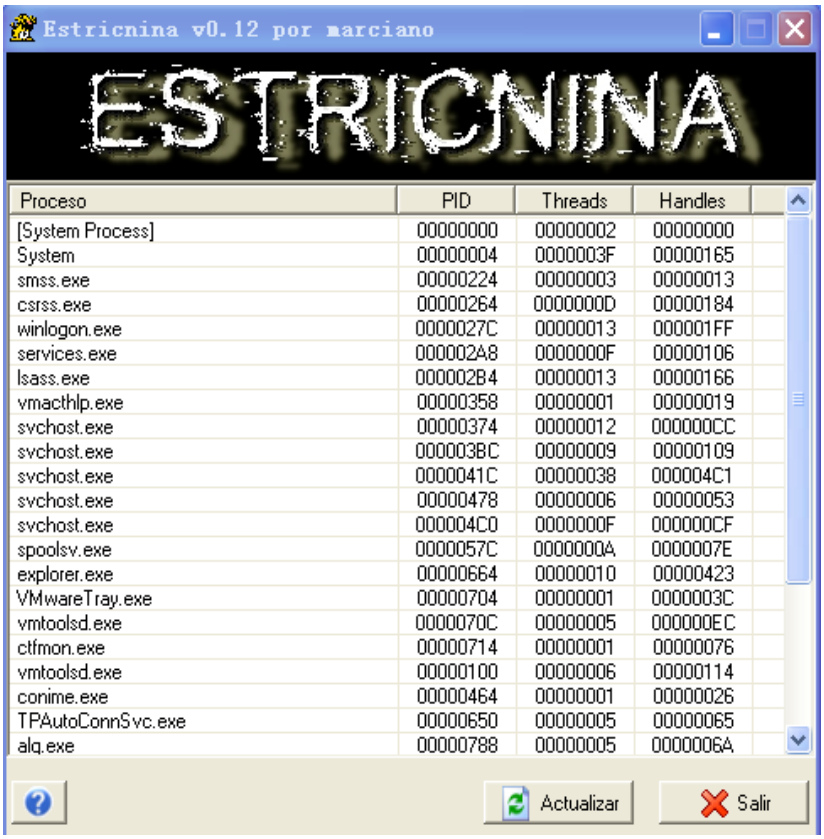
攻击:

我们首先直接运行 UnPackMe_ReCrypt0.80.exe,会发现该程序 CPU 占用率非常高。

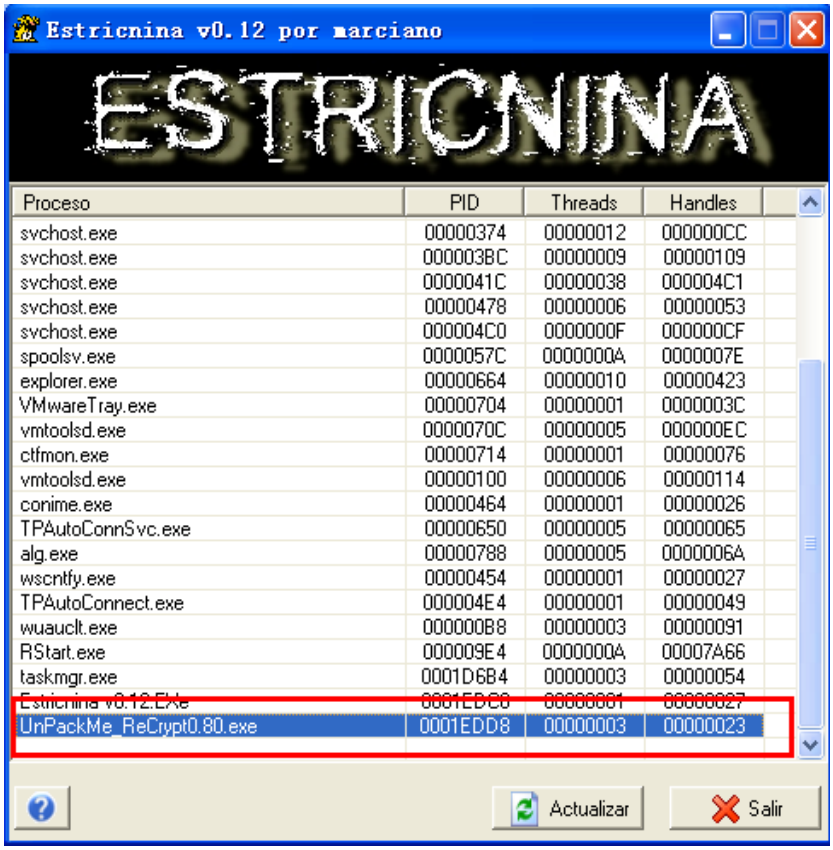


下面我们需要用到 Estricnina 这款工具,使用这款工具我们可以挂起该壳所创建的 3 个线程。(PS:这一步不是必须的,但是挂起这 3 个线程,我们的电脑运行起来会顺畅一些,不会感觉那么卡了)

这里我们打开 Estricnina 主程序。

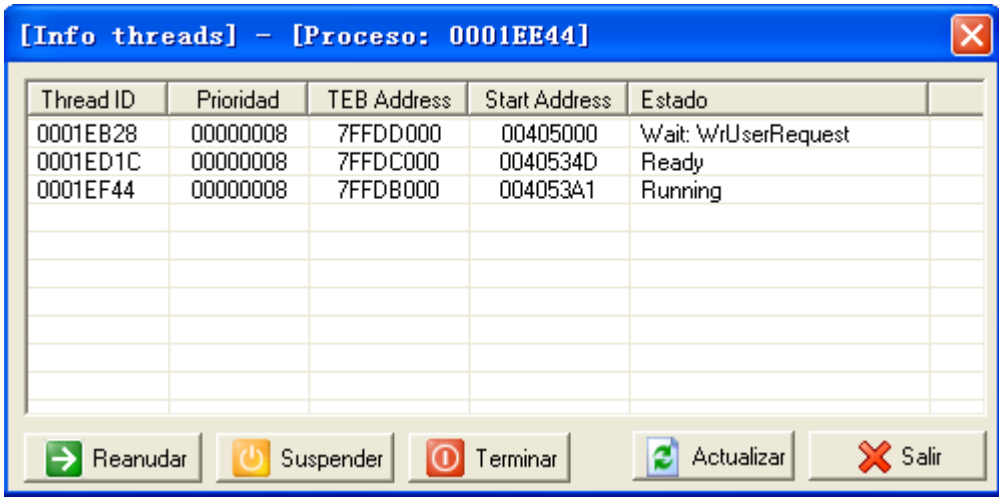


在进程列表中找到 UnPackMe_ReCrypt0.80.exe 对应的进程。

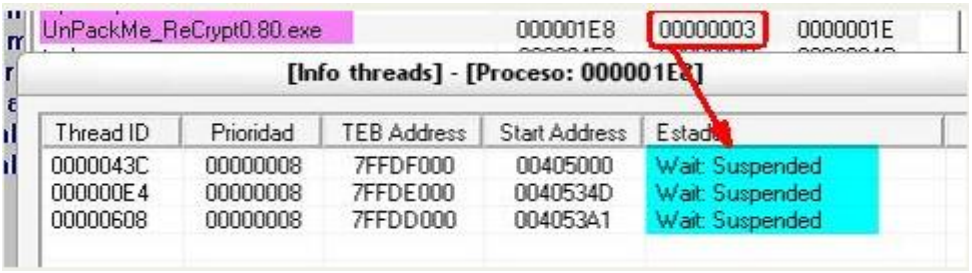


双击之。

可以看到有 3 个线程,分别选中这 3 个线程,并单击下方的 Suspender(挂起)按钮。



我们可以看到这 3 个线程都挂起了。



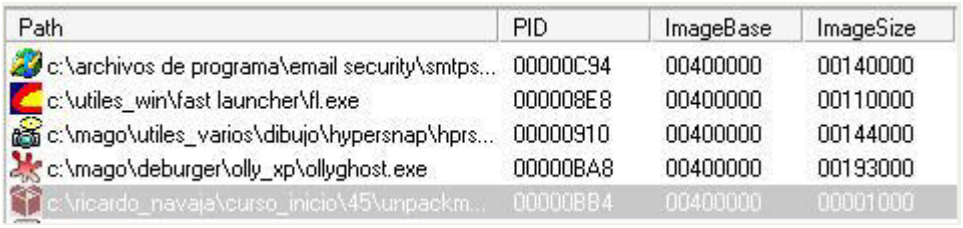
好,这里我们可以看到这 3 个线程都被挂起了,我们再来看看该程序的 CPU 占用率,已经由%99 减到了%0。

现在我们可以顺畅的使用我们的机器了。

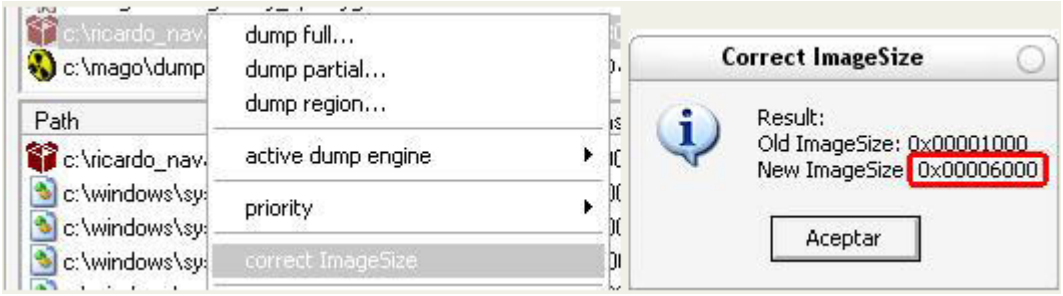
攻击未被检测的内存块

下面我们需要用到 POKEMON 这款工具,通过这款工具我们可以绕过该壳的 Anti Attach(反附加),我们还记得恢复的那个偏移 0xB4 处的 NumOfRvaAndSizes 这个字段的值吧。(其实没有必要恢复 NumOfRvaAndSizes 这个字段的值,恢复它仅仅是为了不让 OD 弹出那个无效 PE 格式的错误框而已)

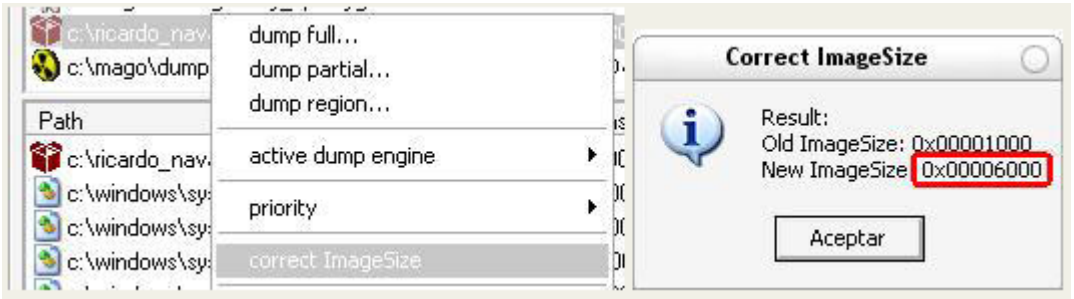
我们选中 UnPackMe_ReCrypt0.80.exe 对应的进程,单击 Anular protection AntiAttach 按钮,会发现那个骷髅头在转动,骷髅头停止转动就表示完毕了。接下来，我们打开 LordPE,定位到 UnPackMe_ReCrypt0.80.exe 所在进程。



我们可以看到 LordPE 的进程列表中显示的 UnPackMe_ReCrypt0.80.exe 所在进程的 ImageSize 为 0x00001000,我们应该还记得该程序的 ImageSize 为 0x00006000 才对呀。这里为了更好的修复 IAT,我们需要将这个 ImageSize 修正。



修复方法:我们在 LordPE 的进程列表窗口中选中 UnPackMe_ReCrypt0.80.exe 对应的进程,单击鼠标右键选择 correct ImageSize。



我们可以看到 ImageSize 已经被成功修复为了 0x00006000。

好了,我们已经搞定了一部分,继续。下面我们使用 OD 附加该进程。我们可以看到弹出了一个错误框提示无效的 PE 格式。

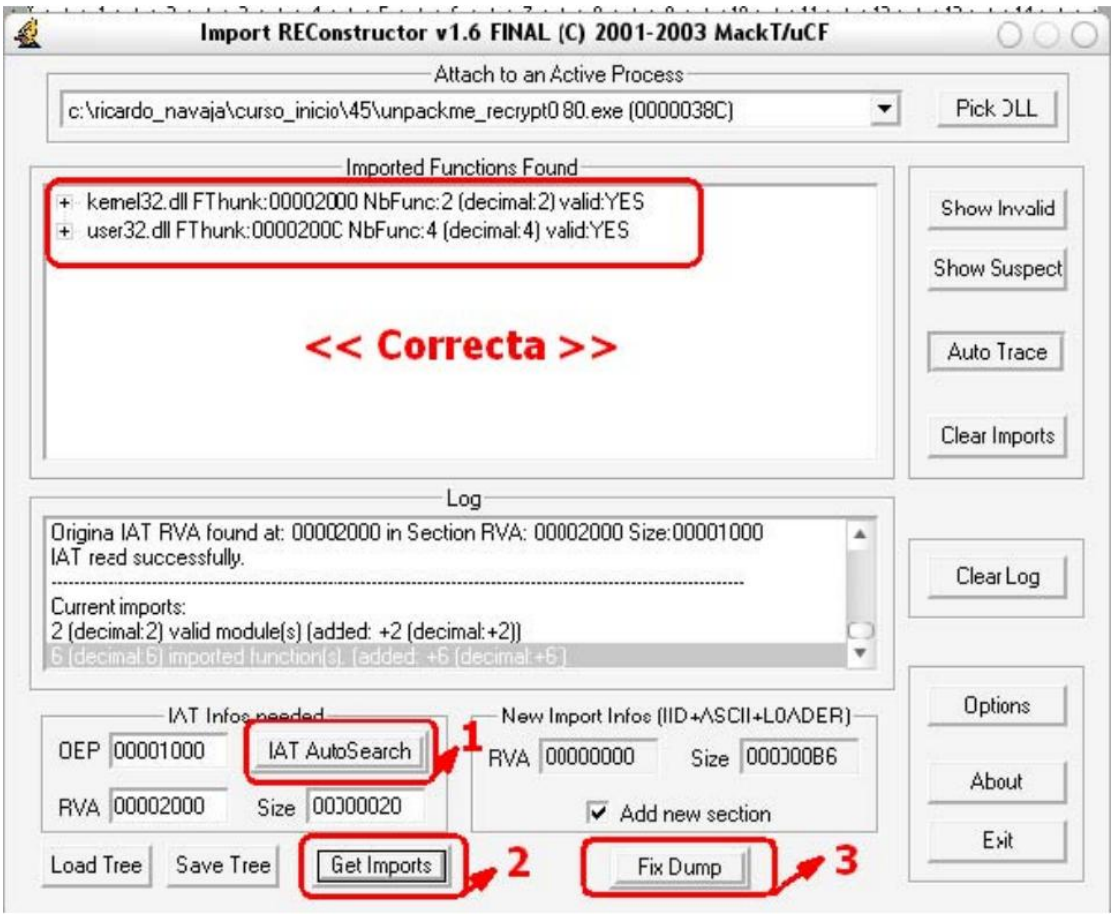
我们单击 Aceptar(西班牙语:确定)按钮。断在了 ntdll.DbgBreakPoint 这个 API 函数中。

我们已经知道了 OEP 为 0x00401000,我们直接在反汇编窗口中单击鼠标右键选择 Go to Expression,输入 401000。

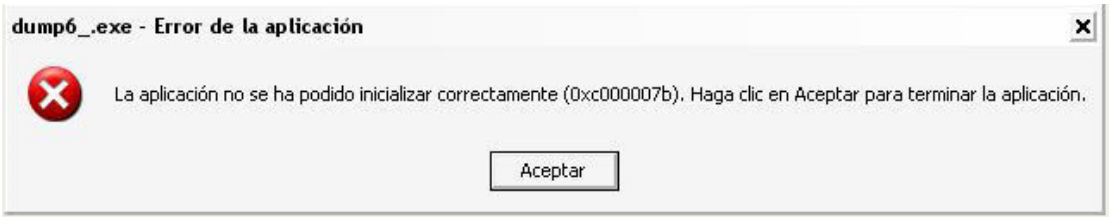
我们可以看到转到了 OEP 处。我们选中第一条指令,单击鼠标右键。

选择 New origin here,将 EIP 的值修改为 0x401000。

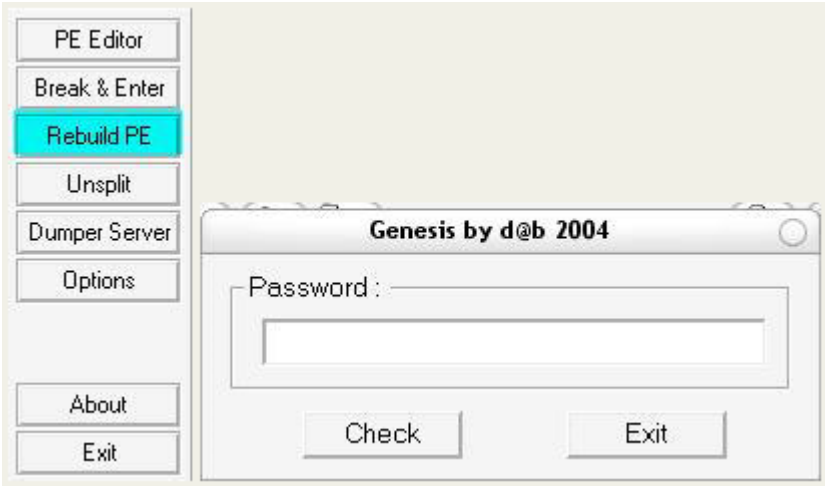
我们可以看到寄存器窗口中的 EIP 寄存器的值已经被修改为了 0x401000,也就是 OEP。现在我们使用 OllyDump 插件来进行 Dump。



首先我们将 OEP 的值填上,接着单击 IAT AutoSearch 按钮,自动定位 IAT。我们可以看到 IAT 已经被定位到了,IAT 起始地址的 RVA 为 0x2000,大小为 0x20，接着我们单击 Get Imports 按钮,获取导入表信息。可以看到获取到的 IAT 项都是有效的.接着单击 Fix Dump 修改刚刚 dump 出来的文件即可。



直接运行修复后的程序,报错了。我们将其拖拽到 LordPE 的 Rebuild PE 按钮上去(重建 PE)。



完美运行。我们再来看一看脱壳后程序的 CPU 占用率。

Nombre de imagen	Nombre de usuario	CPU	Uso de ...
alg.exe	SERVICIO LOCAL	00	3.892 KB
jusched.exe	Perico	00	1.868 KB
WINWORD.EXE	Perico	00	2.012 KB
HprSnap.exe	Perico	00	1.292 KB
agentsvr.exe	Perico	00	1.128 KB
svchost.exe	SYSTEM	00	3.812 KB
nvsvc32.exe	SYSTEM	00	1.868 KB
nod32krn.exe	SYSTEM	00	18.440 KB
explorer.exe	Perico	00	20.412 KB
fl.exe	Perico	00	6.108 KB
WINCMD32.EXE	Perico	00	8.136 KB
spoolsv.exe	SYSTEM	00	4.592 KB
dump6_.exe	Perico	00	3.052 KB
wscntfy.exe	Perico	00	2.472 KB
svchost.exe	SERVICIO LOCAL	00	4.608 KB
svchost.exe	Servicio de red	00	2.632 KB
svchost.exe	SYSTEM	00	18.816 KB
svchost.exe	Servicio de red	00	4.564 KB
svchost.exe	SYSTEM	00	4.484 KB

恩,可以看到 CPU 暂用率为零,搞定。