17bdw随手笔记

- 就职公司：奇安信
- 工作岗位：安全分析师
- 技术方向：渗透测试&应急响应、漏洞分析、安全开发

【逆向工具】使用x64dbg+spy去除WinRAR5.4...

阅览目录

回到顶部

1 学习目标

WinRAR5.40(64位)的弹框广告去除，由于我的系统为x64版本，所以安装了WinRAR（x64）版本。

OD无法调试64位的程序，可以让我熟悉x64dbg进行调试的界面。

其次是这玩意儿真是太蛋疼了，无休止弹广告。

回到顶部

2 破解思路

1）偷梁换柱

修改汇编函数段首为返回值（本次逆向破解采用的方法）

2）NOP掉整个函数内容

回到顶部

3 涉及知识

x64dbg工具快捷键与OD无异

F9：运行

bp CreateWindowExW：在x64dbg底部输入这行命令，对使用CreateWindowExW函数的位置断点。

CreateWindowExW：该函数创建一个层叠式窗口、弹出式窗口或子窗口。参数：

```
HWND CreateWindowEx(
    DWORD DdwExStyle,           //窗口的扩展风格
    LPCTSTR lpClassName,        //指向注册类名的指针
    LPCTSTR lpWindowName,       //指向窗口名称的指针
    DWORD dwStyle,              //窗口风格
    int x,                      //窗口的水平位置
    int y,                      //窗口的垂直位置
    int nWidth,                 //窗口的宽度
    int nHeight,                //窗口的高度
    HWND hWndParent,            //父窗口的句柄
    HMENU hMenu,                //菜单的句柄或是子窗口的标识符
    HINSTANCE hInstance,        //应用程序实例的句柄
    LPVOID lpParam              //指向窗口的创建数据
);
```

回到顶部

4 实现流程

文章档案 (1)
2013年8月(1)
友情链接
卿's Blog
编程备份笔记
最新评论

【软件名称】：WinRar
【软件版本】：5.4
【外壳保护】：无
【操作系统】：Windows 10

既然是弹出窗口，首先要知道弹窗窗口的窗口类名，我使用的是VS2015里自带的工具Spy++ x64。

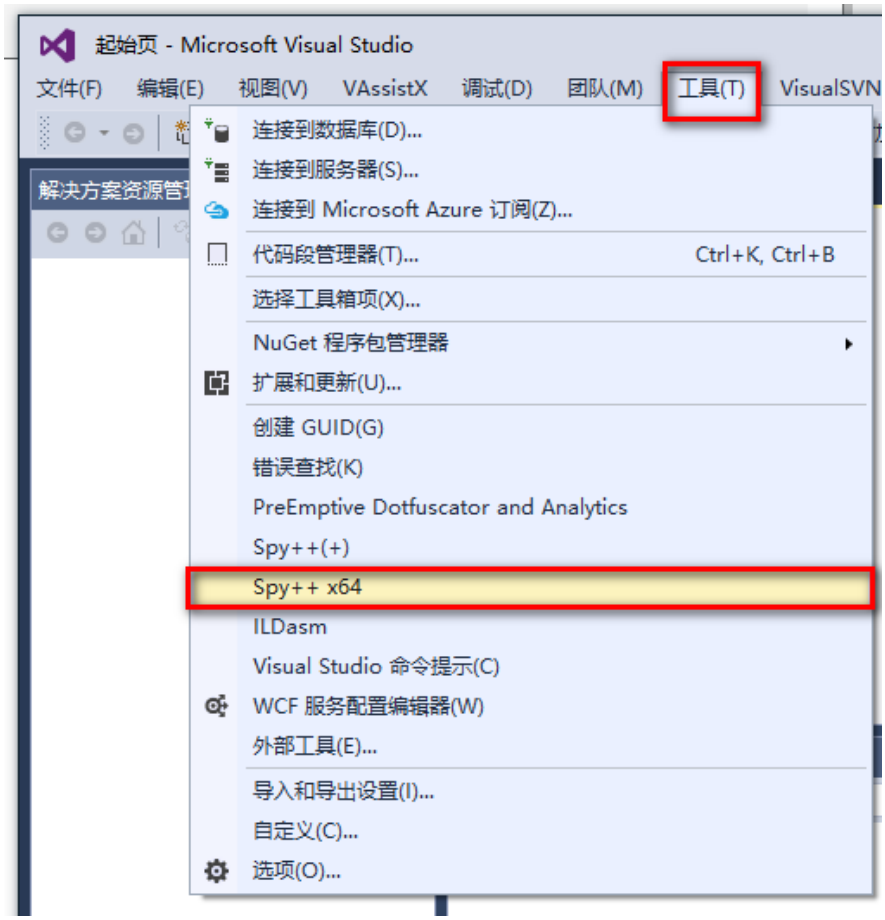

图1 调出Spy++ x64

图2 使用Spy++64查看WinRAR弹出的窗口类名为RarReminder

通过上诉步骤得到WinRAR的类名为RarReminder后，使用x64dbg工具载入WinRAR.exe。在命令的地方使用断点命令【bp CreateWindowExW】，在CreateWindowEx函数断下断点。F9运行到各个断点时观察广告窗口弹出的状态变化。

1. Re:[IDA教程]01-从零开始用IDA做逆向-判断PE文件是32位还是64位、选项卡介绍
@风中小筑 谢谢大佬的教程.受益良多. 惭愧，这类教程大部分是国外的。 我并没有按照所有原句去翻译，都是靠着自己的知识储备去理解和实践然后提炼出来。写得不对的地方还望斧正! 也可以加我微信保持联系，共...
--17bdw

2. Re:【PE结构】PIMAGE_FILE_HEADER中TimeDateStamp的时间戳与标准时间转换
@17bdw 哈哈ok...
--xiaohudie

3. Re:【PE结构】PIMAGE_FILE_HEADER中TimeDateStamp的时间戳与标准时间转换
@xiaohudie 两者格式都不一样啊，同学。...
--17bdw

4. Re:【PE结构】PIMAGE_FILE_HEADER中TimeDateStamp

打赏

图3 使用断点命令【bp CreateWindowExW】

F9运行到出现RarReminder字样的地方，x64dbg这款工具还具备查看断点触发的次数的功能，通过【断点】选项卡看到断点共触发了30次才到这里。

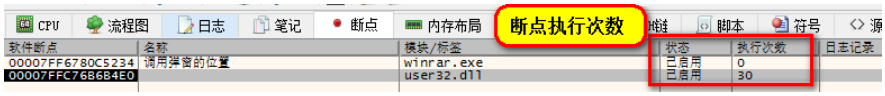

图4 断点触发的次数

在堆栈窗口在call指令的地方按回车键返回到用户层函数。

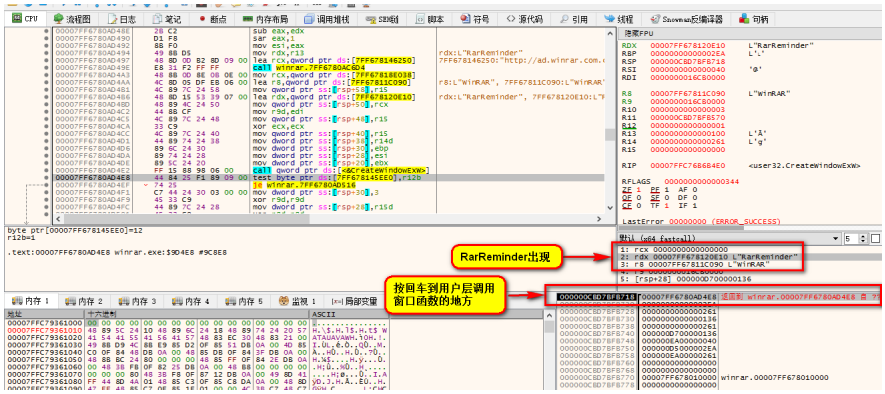

图5 堆栈窗口信息

返回到00007FF6780AD4E8这个地址处，向上看会看到“http://ad.winrar.com.cn/show_40.html?L=7&bl=7&v=540&a=64&src=wrr”这个很明显的广告地址。

汇编函数的代码如下：

```
00007FF6780AD077 | int3                                  |
00007FF6780AD078 | mov qword ptr ss:[rsp+8],rbx          |
00007FF6780AD07D | mov qword ptr ss:[rsp+10],rbp         |
00007FF6780AD082 | mov qword ptr ss:[rsp+18],rsi         |
00007FF6780AD087 | push rdi                              |
00007FF6780AD088 | push r12                              |
00007FF6780AD08A | push r13                              |
00007FF6780AD08C | push r14                              |
00007FF6780AD08E | push r15                              |
```

的时间戳与标准时间转换

好吧 但是这个我没有在winnt中找到--

--xiaohudie

5. Re:【PE结构】PIMAGE_FILE_HEADER中TimeDateStamp的时间戳与标准时间转换

@xiaohudie PE结构里time_t是5个字节 time_t TimeDateStamp...

--17bdw

6. Re:[IDA教程]01-从零开始用IDA做逆向-判断PE文件是32位还是64位、选项卡介绍

谢谢大佬的教程. 受益良多.

--风中小筑

7. Re:【PE结构】PIMAGE_FILE_HEADER中TimeDateStamp的时间戳与标准时间转换

作者，为什么你的时间戳有五个字节呢

--xiaohudie

8. Re:批处理&提权命令

写的很好 学习了 感谢哈

--zpchcbd

打赏

```
00007FF6780AD090 | mov eax,1080                                |
00007FF6780AD095 | call winrar.7FF6780F8BD0                    |
00007FF6780AD09A | sub rsp,rax                                 |
00007FF6780AD09D | mov rax,qword ptr ds:[7FF678148200]         |
00007FF6780AD0A4 | xor rax,rsp                                 |
00007FF6780AD0A7 | mov qword ptr ss:[rsp+1070],rax             |
00007FF6780AD0AF | xor r15d,r15d                               |
00007FF6780AD0B2 | mov sil,cl                                  |
00007FF6780AD0B5 |  cmp byte ptr ds:[7FF67819A204],r15b        |
00007FF6780AD0BC |  je winrar.7FF6780AD0C6                     |
00007FF6780AD0BE |  test dl,dl                                 |
00007FF6780AD0C0 |  je winrar.7FF6780AD55D                     |
00007FF6780AD0C6 |  or rbp,FFFFFFFFFFFFFFFF                    |
00007FF6780AD0CA |  mov r12d,1                                 |
00007FF6780AD0D0 |  cmp dword ptr ds:[7FF678145EE4],r15d       |
00007FF6780AD0D7 |  je winrar.7FF6780AD127                     |
00007FF6780AD0D9 |  mov rcx,r15                                |
00007FF6780AD0DC |  lea rbx,qword ptr ds:[7FF678145ED0]        | 7FF
00007FF6780AD0E3 |  mov r9,r15                                 |
00007FF6780AD0E6 |  mov r8d,480                                |
00007FF6780AD0EC |  xor byte ptr ds:[r9+rbx],cl                |
00007FF6780AD0F0 |  movabs rax,AAAAAAAAAAAAAAAB                |
00007FF6780AD0FA |  mul rcx                                    |
00007FF6780AD0FD |  add rcx,3                                  |
00007FF6780AD101 |  add r9,r12                                 |
00007FF6780AD104 |  shr rdx,1                                  | rdx
00007FF6780AD107 |  add rcx,rdx                                | rdx
00007FF6780AD10A |  and ecx,FFFFFF                             |
00007FF6780AD110 |  cmp r9,r8                                  | r8:
00007FF6780AD113 |  jb winrar.7FF6780AD0EC                     |
00007FF6780AD115 |  cmp dword ptr ds:[7FF678145EE4],r15d       |
00007FF6780AD11C |  je winrar.7FF6780AD1B9                     |
00007FF6780AD122 |  jmp winrar.7FF6780AD1AF                    |
00007FF6780AD127 |  mov ecx,4F8                                |
00007FF6780AD12C |  call winrar.7FF678093F34                   |
00007FF6780AD131 |  mov rbx,rax                                |
00007FF6780AD134 |  cmp word ptr ds:[rax],23                   | 23:
00007FF6780AD138 |  jne winrar.7FF6780AD154                    |
00007FF6780AD13A |  cmp word ptr ds:[rax+2],23                 | 23:
00007FF6780AD13F |  jne winrar.7FF6780AD154                    |
00007FF6780AD141 |  mov rax,rbp                                |
00007FF6780AD144 |  inc rax                                    |
00007FF6780AD147 |  cmp word ptr ds:[rbx+rax*2],r15w           |
00007FF6780AD14C |  jne winrar.7FF6780AD144                    |
00007FF6780AD14E |  cmp rax,64                                 | 64:
00007FF6780AD152 |  jae winrar.7FF6780AD15B                    |
00007FF6780AD154 |  mov rbx,qword ptr ds:[7FF678146350]        | 7FF
00007FF6780AD15B |  mov edi,1000                               |
00007FF6780AD160 |  lea rcx,qword ptr ss:[rsp+70]              |
00007FF6780AD165 |  mov r8d,edi                                |
00007FF6780AD168 |  xor edx,edx                                |
00007FF6780AD16A |  call winrar.7FF6780F9ED0                   |
00007FF6780AD16F |  lea rcx,qword ptr ds:[rbx+4]               |
00007FF6780AD173 |  mov r8d,edi                                |
00007FF6780AD176 |  lea rdx,qword ptr ss:[rsp+70]              |
00007FF6780AD17B |  call winrar.7FF67809CA7C                   |
00007FF6780AD180 |  lea rax,qword ptr ss:[rsp+70]              |
00007FF6780AD185 |  mov r8,rbp                                 |
00007FF6780AD188 |  inc r8                                     | r8:
00007FF6780AD18B |  cmp byte ptr ds:[rax+r8],r15b              |
00007FF6780AD18F |  jne winrar.7FF6780AD188                    |
00007FF6780AD191 |  lea rbx,qword ptr ds:[7FF678145ED0]        | 7FF
```

9. Re:PHPStudy后门事件分析

你这太专业了，同奇安信

--Cleanboys

10. Re:【工具测试】Acunetix 11-登录后扫描的功能

我用的10.5的版本，添加录制登录操作的时候打开不页面时怎么回事呀

--琉璃墨音

11. Re:【移动逆向】对HUAWEI-ManagedProvisioning的一次不完整分析

这就是Android自带的，AOSP里有源码。华为自己定制肯定用华为签名

--Wossoneri

12. Re:【移动逆向】对HUAWEI-ManagedProvisioning的一次不完整分析

@ 代码懒到家但是又不确定是否是恶意程序，所以就分析了下子。...

--17bdw

13. Re:【移动逆向】对HUAWEI-ManagedProvisioning的一次不完整分析

@ 代码懒到家你好，这不是google安卓系统自带的APP程序，它是带了Huawei签名的。...

--17bdw

打赏

```
00007FF6780AD198 |  mov rcx,rbx                                |
00007FF6780AD19B |  lea rdx,qword ptr ss:[rsp+70]              |
00007FF6780AD1A0 |  call winrar.7FF6780AC24C                   |
00007FF6780AD1A5 |  test al,al                                 |
00007FF6780AD1A7 |  jne winrar.7FF6780AD1B9                    |
00007FF6780AD1A9 |  mov r8d,480                                |
00007FF6780AD1AF |  xor edx,edx                                |
00007FF6780AD1B1 |  mov rcx,rbx                                |
00007FF6780AD1B4 |  call winrar.7FF6780F9ED0                   |
00007FF6780AD1B9 |  cmp byte ptr ds:[7FF6781857E4],r15b        |
00007FF6780AD1C0 |  jne winrar.7FF6780AD1CE                    |
00007FF6780AD1C2 |  cmp dword ptr ds:[7FF678158474],28         | 28:
00007FF6780AD1C9 |  mov dil,r12b                               |
00007FF6780AD1CC |  ja winrar.7FF6780AD1D1                     |
00007FF6780AD1CE |  mov dil,r15b                               |
00007FF6780AD1D1 |  test sil,sil                               |
00007FF6780AD1D4 |  je winrar.7FF6780AD528                     |
00007FF6780AD1DA |  call winrar.7FF678078ECC                   |
00007FF6780AD1DF |  cmp eax,501                                |
00007FF6780AD1E4 |  ja winrar.7FF6780AD1F6                     |
00007FF6780AD1E6 |  test dword ptr ds:[7FF678145EE0],200       |
00007FF6780AD1F0 |  je winrar.7FF6780AD55D                     |
00007FF6780AD1F6 |  cmp byte ptr ds:[7FF678146250],r15b        | 7FF
00007FF6780AD1FD |  je winrar.7FF6780AD55D                     |
00007FF6780AD203 |  mov byte ptr ds:[7FF678145FFB],r15b        |
00007FF6780AD20A |  mov byte ptr ds:[7FF6781460FF],r15b        |
00007FF6780AD211 |  mov byte ptr ds:[7FF67814634F],r15b        |
00007FF6780AD218 |  test dil,dil                               |
00007FF6780AD21B |  jne winrar.7FF6780AD22F                    |
00007FF6780AD21D |  mov al,byte ptr ds:[7FF678145EE0]          |
00007FF6780AD223 |  and al,80                                  |
00007FF6780AD225 |  neg al                                     |
00007FF6780AD227 |  sbb eax,eax                                |
00007FF6780AD229 |  and dword ptr ds:[7FF678145EE8],eax        |
00007FF6780AD22F |  cmp dword ptr ds:[7FF678145EF8],r15d       |
00007FF6780AD236 |  lea rbp,qword ptr ds:[7FF678146250]        | 7FF
00007FF6780AD23D |  mov bl,r15b                                |
00007FF6780AD240 |  lea rsi,qword ptr ds:[7FF67811BA38]        | 7FF
00007FF6780AD247 |  mov r13d,100                               |
00007FF6780AD24D |  jbe winrar.7FF6780AD2A1                    |
00007FF6780AD24F |  cmp byte ptr ds:[7FF6781857E4],r15b        |
00007FF6780AD256 |  jne winrar.7FF6780AD2A1                    |
00007FF6780AD258 |  xor r8d,r8d                                |
00007FF6780AD25B |  lea rdx,qword ptr ds:[7FF678120DC8]        | rdx
00007FF6780AD262 |  mov rcx,rsi                                |
00007FF6780AD265 |  call winrar.7FF6780AB6AC                   |
00007FF6780AD26A |  cmp eax,dword ptr ds:[7FF678145EF8]        |
00007FF6780AD270 |  jae winrar.7FF6780AD2A1                    |
00007FF6780AD272 |  lea r8d,dword ptr ds:[rax+1]               |
00007FF6780AD276 |  mov rcx,rsi                                |
00007FF6780AD279 |  lea rdx,qword ptr ds:[7FF678120DC8]        | rdx
00007FF6780AD280 |  call winrar.7FF6780AC210                   |
00007FF6780AD285 |  cmp byte ptr ds:[7FF678145EFC],r15b        | 7FF
00007FF6780AD28C |  mov bl,r12b                                |
00007FF6780AD28F |  je winrar.7FF6780AD34E                     |
00007FF6780AD295 |  lea rdx,qword ptr ds:[7FF678145EFC]        | rdx
00007FF6780AD29C |  jmp winrar.7FF6780AD343                    |
00007FF6780AD2A1 |  cmp dword ptr ds:[7FF678145FFC],r15d       |
00007FF6780AD2A8 |  jbe winrar.7FF6780AD2F1                    |
00007FF6780AD2AA |  test dil,dil                               |
00007FF6780AD2AD |  je winrar.7FF6780AD2F1                     |
00007FF6780AD2AF |  xor r8d,r8d                                |
```

14. Re:【移动逆向】对HUAWEI-ManagedProvisioning的一次不完整分析

你好，这个不是google安卓系统自带的一个app程序么？为什么是恶意病毒程序呢?

--代码懒到家

15. Re:【网络编程4】网络编程基础-ARP响应（ARP欺骗之中间人攻击）

求源码~

--Elevean

16. Re:【网络编程4】网络编程基础-ARP响应（ARP欺骗之中间人攻击）

你可以把arp欺骗的工程发给我吗

--Duke777

打赏

```
00007FF6780AD2B2 |  lea rdx,qword ptr ds:[7FF678120DE0]     | rdx
00007FF6780AD2B9 |  mov rcx,rsi                            |
00007FF6780AD2BC |  call winrar.7FF6780AB6AC               |
00007FF6780AD2C1 |  cmp eax,dword ptr ds:[7FF678145FFC]    |
00007FF6780AD2C7 |  jae winrar.7FF6780AD2F1                |
00007FF6780AD2C9 |  lea r8d,dword ptr ds:[rax+1]           |
00007FF6780AD2CD |  mov rcx,rsi                            |
00007FF6780AD2D0 |  lea rdx,qword ptr ds:[7FF678120DE0]     | rdx
00007FF6780AD2D7 |  call winrar.7FF6780AC210               |
00007FF6780AD2DC |  cmp byte ptr ds:[7FF678146000],r15b    | 7FF
00007FF6780AD2E3 |  mov bl,r12b                            |
00007FF6780AD2E6 |  je winrar.7FF6780AD34E                 |
00007FF6780AD2E8 |  lea rdx,qword ptr ds:[7FF678146000]    | rdx
00007FF6780AD2EF |  jmp winrar.7FF6780AD343                |
00007FF6780AD2F1 |  cmp dword ptr ds:[7FF678146100],r15d   |
00007FF6780AD2F8 |  jbe winrar.7FF6780AD34E                |
00007FF6780AD2FA |  cmp byte ptr ds:[7FF6781857E4],r15b    |
00007FF6780AD301 |  je winrar.7FF6780AD34E                 |
00007FF6780AD303 |  xor r8d,r8d                            |
00007FF6780AD306 |  lea rdx,qword ptr ds:[7FF678120DF8]    | rdx
00007FF6780AD30D |  mov rcx,rsi                            |
00007FF6780AD310 |  call winrar.7FF6780AB6AC               |
00007FF6780AD315 |  cmp eax,dword ptr ds:[7FF678146100]    |
00007FF6780AD31B |  jae winrar.7FF6780AD34E                |
00007FF6780AD31D |  lea r8d,dword ptr ds:[rax+1]           |
00007FF6780AD321 |  mov rcx,rsi                            |
00007FF6780AD324 |  lea rdx,qword ptr ds:[7FF678120DF8]    | rdx
00007FF6780AD32B |  call winrar.7FF6780AC210               |
00007FF6780AD330 |  cmp byte ptr ds:[7FF678146104],r15b    |
00007FF6780AD337 |  mov bl,r12b                            |
00007FF6780AD33A |  je winrar.7FF6780AD34E                 |
00007FF6780AD33C |  lea rdx,qword ptr ds:[7FF678146104]    | rdx
00007FF6780AD343 |  mov r8,r13                             | r8:
00007FF6780AD346 |  mov rcx,rbp                            |
00007FF6780AD349 |  call winrar.7FF678099E48               |
00007FF6780AD34E |  call qword ptr ds:[<&GetTickCount>]    |
00007FF6780AD354 |  mov ecx,eax                            |
00007FF6780AD356 |  mov eax,10624DD3                       |
00007FF6780AD35B |  mul ecx                                |
00007FF6780AD35D |  mov eax,edx                            |
00007FF6780AD35F |  shr eax,6                              |
00007FF6780AD362 |  cmp byte ptr ds:[7FF6781857E4],r15b    |
00007FF6780AD369 |  je winrar.7FF6780AD382                 |
00007FF6780AD36B |  mov ecx,dword ptr ds:[7FF678145EF4]    |
00007FF6780AD371 |  test ecx,ecx                           |
00007FF6780AD373 |  je winrar.7FF6780AD3B2                 |
00007FF6780AD375 |  xor edx,edx                            |
00007FF6780AD377 |  div ecx                                |
00007FF6780AD379 |  test edx,edx                           |
00007FF6780AD37B |  jne winrar.7FF6780AD3B2                |
00007FF6780AD37D |  mov bl,r12b                            |
00007FF6780AD380 |  jmp winrar.7FF6780AD3B2                |
00007FF6780AD382 |  test dil,dil                           |
00007FF6780AD385 |  jne winrar.7FF6780AD39B                |
00007FF6780AD387 |  mov ecx,dword ptr ds:[7FF678145EEC]    |
00007FF6780AD38D |  test ecx,ecx                           |
00007FF6780AD38F |  je winrar.7FF6780AD3B2                 |
00007FF6780AD391 |  xor edx,edx                            |
00007FF6780AD393 |  div ecx                                |
00007FF6780AD395 |  test edx,edx                           |
00007FF6780AD397 |  jne winrar.7FF6780AD3B2                |
00007FF6780AD399 |  jmp winrar.7FF6780AD3BA                |
```

```
00007FF6780AD39B |  mov ecx,dword ptr ds:[7FF678145EF0]     |
00007FF6780AD3A1 |  test ecx,ecx                           |
00007FF6780AD3A3 |  je winrar.7FF6780AD3B2                 |
00007FF6780AD3A5 |  xor edx,edx                            |
00007FF6780AD3A7 |  movzx ebx,bl                           |
00007FF6780AD3AA |  div ecx                                |
00007FF6780AD3AC |  test edx,edx                           |
00007FF6780AD3AE |  cmove ebx,r12d                         |
00007FF6780AD3B2 |  test bl,bl                             |
00007FF6780AD3B4 |  je winrar.7FF6780AD55D                 |
00007FF6780AD3BA |  test byte ptr ds:[7FF678145EE0],2      |
00007FF6780AD3C1 |  mov edi,16C80000                       |
00007FF6780AD3C6 |  mov eax,16CC0000                       |
00007FF6780AD3CB |  cmove edi,eax                          |
00007FF6780AD3CE |  test byte ptr ds:[7FF678145EE0],8      |
00007FF6780AD3D5 |  jne winrar.7FF6780AD3DD                |
00007FF6780AD3D7 |  or edi,30000                           |
00007FF6780AD3DD |  mov ecx,dword ptr ds:[7FF678146208]    |
00007FF6780AD3E3 |  mov ebx,80000000                       |
00007FF6780AD3E8 |  mov esi,ebx                            |
00007FF6780AD3EA |  mov ebp,ebx                            |
00007FF6780AD3EC |  mov r14d,ebx                           |
00007FF6780AD3EF |  test ecx,ecx                           |
00007FF6780AD3F1 |  je winrar.7FF6780AD494                 |
00007FF6780AD3F7 |  cmp dword ptr ds:[7FF678146204],r15d   |
00007FF6780AD3FE |  je winrar.7FF6780AD494                 |
00007FF6780AD404 |  call winrar.7FF6780D08F8               |
00007FF6780AD409 |  mov ecx,21                             | 21:
00007FF6780AD40E |  mov ebx,eax                            |
00007FF6780AD410 |  call qword ptr ds:[<&GetSystemMetrics>] |
00007FF6780AD416 |  mov ecx,4                              |
00007FF6780AD41B |  lea esi,dword ptr ds:[rbx+rax*2]       |
00007FF6780AD41E |  call qword ptr ds:[<&GetSystemMetrics>] |
00007FF6780AD424 |  add esi,eax                            |
00007FF6780AD426 |  mov eax,dword ptr ds:[7FF678145EE0]    |
00007FF6780AD42C |  test al,40                             |
00007FF6780AD42E |  jne winrar.7FF6780AD435                |
00007FF6780AD430 |  test r13d,eax                          |
00007FF6780AD433 |  jne winrar.7FF6780AD43B                |
00007FF6780AD435 |  add esi,dword ptr ds:[7FF67819A200]    |
00007FF6780AD43B |  mov ecx,dword ptr ds:[7FF678146204]    |
00007FF6780AD441 |  call winrar.7FF6780D088C               |
00007FF6780AD446 |  mov ecx,20                             | 20:
00007FF6780AD44B |  mov ebx,eax                            |
00007FF6780AD44D |  call qword ptr ds:[<&GetSystemMetrics>] |
00007FF6780AD453 |  xor edx,edx                            |
00007FF6780AD455 |  lea r8,qword ptr ss:[rsp+60]           |
00007FF6780AD45A |  xor r9d,r9d                            |
00007FF6780AD45D |  lea ebx,dword ptr ds:[rbx+rax*2]       |
00007FF6780AD460 |  lea ecx,dword ptr ds:[rdx+30]          | rdx
00007FF6780AD463 |  call qword ptr ds:[<&SystemParametersIn |
00007FF6780AD469 |  mov eax,dword ptr ss:[rsp+68]          |
00007FF6780AD46D |  cmp ebx,eax                            |
00007FF6780AD46F |  mov ebp,eax                            |
00007FF6780AD471 |  cmovl ebp,ebx                          |
00007FF6780AD474 |  sub eax,ebp                            |
00007FF6780AD476 |  cdq                                    |
00007FF6780AD477 |  sub eax,edx                            |
00007FF6780AD479 |  sar eax,1                              |
00007FF6780AD47B |  mov ebx,eax                            |
00007FF6780AD47D |  mov eax,dword ptr ss:[rsp+6C]          |
00007FF6780AD481 |  cmp esi,eax                            |
```

```
00007FF6780AD483 |  mov r14d,eax                                |
00007FF6780AD486 |  cmovl r14d,esi                              |
00007FF6780AD48A |  sub eax,r14d                                |
00007FF6780AD48D |  cdq                                         |
00007FF6780AD48E |  sub eax,edx                                 |
00007FF6780AD490 |  sar eax,1                                   |
00007FF6780AD492 |  mov esi,eax                                 |
00007FF6780AD494 |  mov rdx,r13                                 | rdx
00007FF6780AD497 |  lea rcx,qword ptr ds:[7FF678146250]         | 7FF
00007FF6780AD49E |  call winrar.7FF6780AC6D4                    |
00007FF6780AD4A3 |  mov rcx,qword ptr ds:[7FF67818E038]         |
00007FF6780AD4AA |  lea r8,qword ptr ds:[7FF67811C090]          | r8:
00007FF6780AD4B1 |  mov qword ptr ss:[rsp+58],r15               |
00007FF6780AD4B6 |  lea rdx,qword ptr ds:[7FF678120E10]         | rdx
00007FF6780AD4BD |  mov qword ptr ss:[rsp+50],rcx               |
00007FF6780AD4C2 |  mov r9d,edi                                 |
00007FF6780AD4C5 |  mov qword ptr ss:[rsp+48],r15               |
00007FF6780AD4CA |  xor ecx,ecx                                 |
00007FF6780AD4CC |  mov qword ptr ss:[rsp+40],r15               |
00007FF6780AD4D1 |  mov dword ptr ss:[rsp+38],r14d              |
00007FF6780AD4D6 |  mov dword ptr ss:[rsp+30],ebp               |
00007FF6780AD4DA |  mov dword ptr ss:[rsp+28],esi               |
00007FF6780AD4DE |  mov dword ptr ss:[rsp+20],ebx               |
00007FF6780AD4E2 |  call qword ptr ds:[<&CreateWindowExW>]      |
00007FF6780AD4E8 |  test byte ptr ds:[7FF678145EE0],r12b        |
00007FF6780AD4EF |  je winrar.7FF6780AD516                      |
00007FF6780AD4F1 |  mov dword ptr ss:[rsp+30],3                 |
00007FF6780AD4F9 |  xor r9d,r9d                                 |
00007FF6780AD4FC |  mov dword ptr ss:[rsp+28],r15d              |
00007FF6780AD501 |  xor r8d,r8d                                 |
00007FF6780AD504 |  or rdx,FFFFFFFFFFFFFFFF                     | rdx
00007FF6780AD508 |  mov dword ptr ss:[rsp+20],r15d              |
00007FF6780AD50D |  mov rcx,rax                                 |
00007FF6780AD510 |  call qword ptr ds:[<&SetWindowPos>]         |
00007FF6780AD516 |  cmp qword ptr ds:[7FF678158370],r15         |
00007FF6780AD51D |  je winrar.7FF6780AD55D                      |
00007FF6780AD51F |  mov byte ptr ds:[7FF67819A204],r12b         |
00007FF6780AD526 |  jmp winrar.7FF6780AD55D                     |
00007FF6780AD528 |  test dil,dil                                |
00007FF6780AD52B |  je winrar.7FF6780AD55D                      |
00007FF6780AD52D |  mov byte ptr ds:[7FF67819A204],r12b         |
00007FF6780AD534 |  call qword ptr ds:[<&GetFocus>]             |
00007FF6780AD53A |  mov rcx,qword ptr ds:[7FF67818E030]         |
00007FF6780AD541 |  lea r9,qword ptr ds:[7FF6780E0BFC]          |
00007FF6780AD548 |  mov r8,rax                                  | r8:
00007FF6780AD54B |  mov qword ptr ss:[rsp+20],r15               |
00007FF6780AD550 |  lea rdx,qword ptr ds:[7FF678120E28]         | rdx
00007FF6780AD557 |  call qword ptr ds:[<&DialogBoxParamW>]      |
00007FF6780AD55D |  mov rcx,qword ptr ss:[rsp+1070]             |
00007FF6780AD565 |  xor rcx,rsp                                 |
00007FF6780AD568 |  call winrar.7FF6780F8C40                    |
00007FF6780AD56D |  lea r11,qword ptr ss:[rsp+1080]             |
00007FF6780AD575 |  mov rbx,qword ptr ds:[r11+30]               |
00007FF6780AD579 |  mov rbp,qword ptr ds:[r11+38]               |
00007FF6780AD57D |  mov rsi,qword ptr ds:[r11+40]               |
00007FF6780AD581 |  mov rsp,r11                                 |
00007FF6780AD584 |  pop r15                                     |
00007FF6780AD586 |  pop r14                                     |
00007FF6780AD588 |  pop r13                                     |
00007FF6780AD58A |  pop r12                                     |
00007FF6780AD58C |  pop rdi                                     |
00007FF6780AD58D |  ret                                         |
```

可以看到函数头部地址为：00007FF6780AD078 | mov qword ptr ss:[rsp+8],rbx
函数尾部地址为：ret
修改之后，函数头部地址为：00007FF6780AD078 | ret

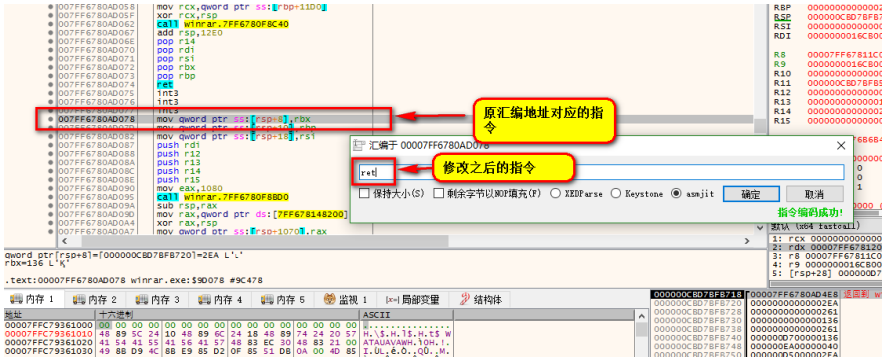

图6 修改函数头部反汇编指令

修改之后，鼠标右键选择补丁-修补文件。

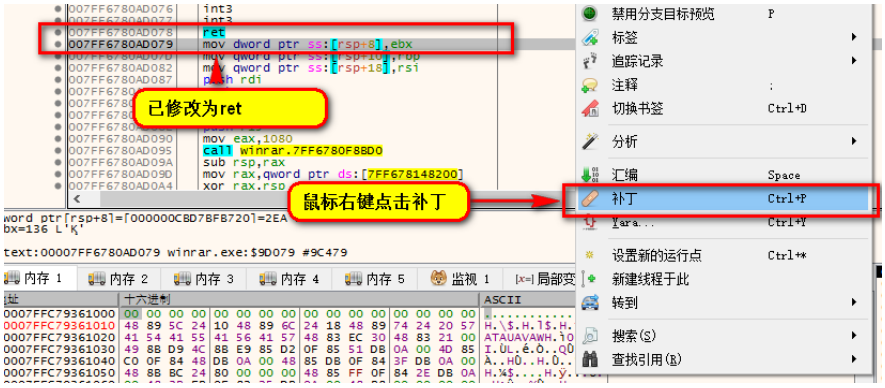

图7 选择补丁

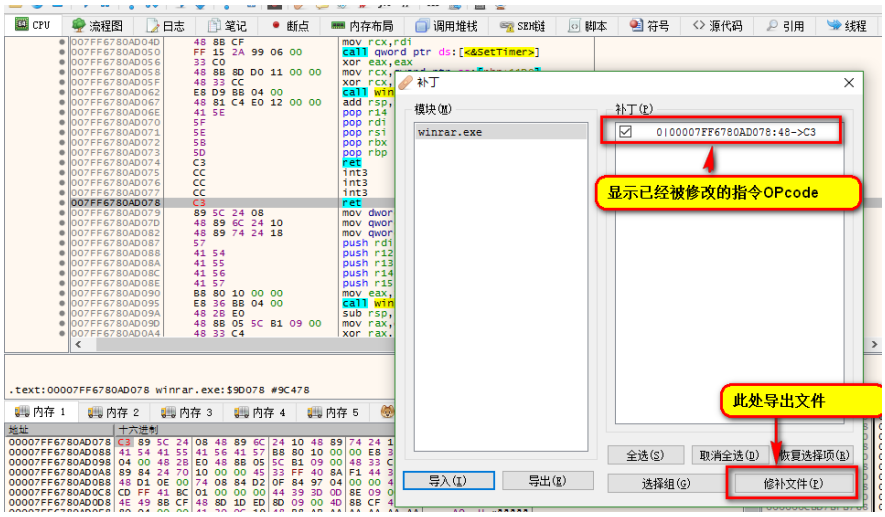

图8 修补文件

小功告成！再次打开rar弹窗广告已经消失了。可是评估版本字样还在，追求完美可以选择使用资源管理工具去除字样。

图9 去除弹窗

我使用了Restorator这款资源修改软件，不过使用这款软件的少侠们可就小心了。因为这款资源软件会自动修改.exe扩展名的关联，**请切记在虚拟机下运行。**

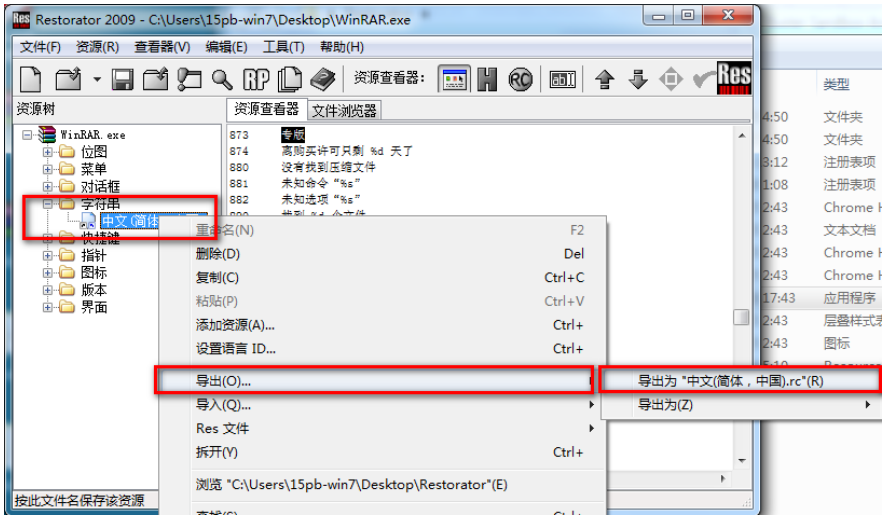

图10 导出资源文件.rc

导出资源文件.rc后，用notepad++打开.rc后缀的文件。修改【评估版本】为你想要修改的文字。然后再导入到资源中。操作比较简单，就不赘述了！

图11 大功告成!

回到顶部

5 参考文章

winrar 5.4 去广告教程
http://www.xuepojie.com/thread-29596-1-1.html
Winrar 5.30 X64去广告
http://www.52pojie.cn/thread-449909-1-1.html
WinRAR 5.31 x64去广告破解
http://blog.csdn.net/u011138447/article/details/52140202

装了Restorator，打开应用程序，提示不支持此接口的解决方法
http://blog.csdn.net/redzqin/article/details/8664290

分类: common-二进制基础

« 上一篇： 【工具】大量病毒样本取样工作经验1（重复样本排除、分析方法）
» 下一篇： 【黑客免杀攻防】读书笔记3 - 花指令在免杀中的应用

posted @ 2017-07-23 01:46 17bdw 阅读(1403) 评论(0) 编辑 收藏