链滴

160CrackMe 之 001

作者：livisun

原文链接：https://ld246.com/article/1604307724316

来源网站：链滴

<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/bing/20190720.jpg?imageView2/1/w/960/h/540/interlace/1/q/100">
<blockquote>
本系列博客，从一个完全没有经验的逆向小白的角度出发，尝试搞定 160 个 CrackMe，博客将本按照如下流程进行：

环境和工具介绍（不同的运行环境，不同的工具，甚至不同的版本都可能造成操作方法、执行细和运行结果的差异。遇到问题，请考虑运行环境等问题，自行百度研究或者和我研究讨论）；
程序分析（破解之前，我们必须尽可能的去了解程序，例如程序的开发语言、加壳加密情况、PE结构、执行流程等，分析作者的开发思路，有助于我们发现破解的关键点）；
破解思路和破解流程（破解一个程序方法往往有很多种，如何找到最好，最快的一种，往往需要足够的经验、敏锐的洞察能力和高超的思维逻辑。真正的高手一定是在思维逻辑上碾压对手，不过这我们先看看一个菜鸟的思维逻辑）；
如果可以写出注册机（暴力破解也许能达到效果，但是那不是我们追求的，我们不光要做到，还做好做漂亮）。

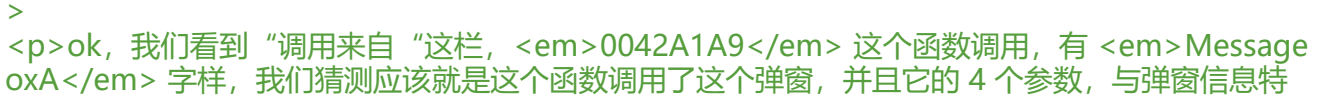
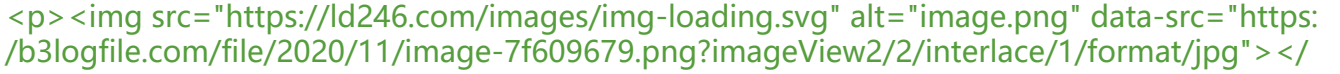
160 个 CrackMe 下载链接 <a href="https://ld246.com/forward?goto=https%3A%2F%2Fliv
sun.cowtransfer.com%2Fs%2F2187fdba96614a" target="_blank" rel="nofollow ugc">https://li
isun.cowtransfer.com/s/2187fdba96614a。
</blockquote>
<h2 id="1--环境和工具">1. 环境和工具</h2>

win7 SP1
画眉专用 OD v2.0 （<a href="https://ld246.com/forward?goto=https%3A%2F%2Flivisun.c
wtransfer.com%2Fs%2Fb94d32c237ca4c" target="_blank" rel="nofollow ugc">https://livisun.
owtransfer.com/s/b94d32c237ca4c）
DIE v1.01（<a href="https://ld246.com/forward?goto=https%3A%2F%2Flivisun.cowtrans
er.com%2Fs%2F8f7fa56c40bd4e" target="_blank" rel="nofollow ugc">https://livisun.cowtrans
er.com/s/8f7fa56c40bd4e）

<blockquote>
注：正常逆向程序，应该在虚拟机里进行破解，防止作者加了一点奇怪的反调试，导致格盘、死或者蓝屏等，不过既然是 CrackMe，还是被各路大神蹂躏多年的 应该不会有这种骚暗桩。（其实我是偷懒直接在物理机上跑的）。
</blockquote>
<h2 id="2-程序分析">2.程序分析</h2>
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/11/image-66b09b78.png?imageView2/2/interlace/1/format/jpg"><
p>

首先不管三七二十一，先把程序跑起来再说（很多时候，某些程序并不能正确运行在你现在的电环境上，跑都跑不起来就先别考虑别的了），映入眼帘的是一个烦人的欢迎界面，好了那我们首先就要去掉这个弹窗；
然后我们到处点点，发现这个程序主要有两个功能：一个是 Serial/Name，需要输入用户名和注码才能通过，输入伪码，点击 Check it Baby!，它会弹出一个错误提示框：Sorr
， The Serial is incorrect !，另外一个 Serial 只需要输入一个注册码，我们也输入一个伪码一样弹出一个错误提示框：Try Again！；
丢到 DIE 里面看一下，是一个 Delphi 程序，无壳。

<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/11/image-86f7e216.png?imageView2/2/interlace/1/format/jpg"></
>
<h2 id="3-破解思路及流程">3.破解思路及流程</h2>
<h2 id="1-先把弹窗和去掉">1、先把弹窗和去掉</h2>

我们把程序拖入 OD，程序停在 OEP，按 F9，让程序直接跑起来。
我们知道，程序跑起来应该弹窗，（但是一点提示都没有，把 OD 最小化，我才看到这个提示，还以为出什么毛病了呢，坑爹），既然有弹窗，那我们就可以用暂停大法，打开调用堆栈，找到执行窗的位置，nop 掉它。
<blockquote>
注：程序弹窗，这里指的是模态弹窗，即程序执行流程被挂起，必须处理这个弹窗，否则父窗口法选中，而非模态弹窗，则是可以选中父窗口，甚至不处理弹窗，继续执行程序流程；因此在模态窗下暂停，打开调用堆栈就能看到当前程序的调用过程了。
</blockquote>
好，我们看下我们的思路可不可行，按 F12 暂停程序，接着 Alt+K，打开调用堆栈。

ok，我们看到“调用来自“这栏，0042A1A9 这个函数调用，有 MessageoxA 字样，我们猜测应该就是这个函数调用了这个弹窗，并且它的 4 个参数，与弹窗信息特吻合（7637FDC1 也有这样的特征，但是我们知道，调用顺序应该是由下往上，这个址太大，明显是在系统领空，所以我们找 0042A1A9 位置），鼠标放到这条记录上，开右键菜单，选择显示调用，我们就回到了弹窗的调用位置。

我们 Ctrl+F2，重新运行，然后 Ctrl+G ，找到“0042A1A9”，然后，右键——> 二进制—> 用 NOP 填充，然后我们再按 F9，运行，OK，弹窗没有了。
接着我们把修改保存一下（OD 可能会把你的修改给重置掉，比如当你 Ctrl+F2 重新运行的时候为了避免麻烦，通常成功修改一部分就先保存一个版本，然后接着破解），右键——> 复制到可行文件——> 所有修改——> 全部复制，然后在弹出的新界面中，右键——> 保存文件，个名字例如 Acid burn1.exe（这里如果选择直接修改的话，需要手动把修改部分选中）。
<blockquote>
这篇博客是该系列第一篇，所以我把某些操作细节都写了下来，方便与我水平一样的菜鸟可以一学习，随着系列文章的更新，介绍过的操作，就不会在讲了。
</blockquote>

<h2 id="2-破解-Serial-Name">2、破解 Serial/Name</h2>
将修改过的程序拖进 OD，F9，跑起来，现在来到主窗口，点击 “Serial/Name“按钮，输入伪：
Name：livisun
Serial：12345678（这里需要提一下，虽然伪码市瞎写的，但是最好不要填空，不要过短和过，因为有些程序，可能会检查这个输入，一会儿跟踪的时候，走进一些检查的 call 里面去，增加不必的麻烦）。
我们知道，伪码输入点击“Check it Baby!”后，会弹出提示窗口，有弹窗，我们就可以用“暂大法”去定位，不过我们也可以通过 win32 API 下断来定位关键点。
我们知道，弹窗的 API 有 MessageBoxA、MessageBoxW、MessageBoxExA 和 MessageBoxW，（他们的关系请自行百度） Ctrl+G 打开表达式窗口，输入 “MessageBoxA”，回车，F2 下。
<blockquote>
注：

一般来说 我们会下 MessageBoxA，如果断不下来我 MessageBoxW 也下，然后是 MessageBxExA 或者 MessageBoxExW；
通过 Ctrl+G 搜索 API 这种方式适合记不住 API 拼写或者大小写的，我们也可以在 OD 的左下角 Command 命令行 输入 bpx MessageBoxA，直接下断（我看到很多教程 使用 bp MessageboxA 来下断，bp 和 bpx 的区别在哪里呢，bp 会断在 MessageBoxA 函数的入口，而 bpx 则

</blockquote>

断在代码段所有调用 MessageBoxA 函数的代码位置，所以直接使用 bpx 就不用先进系统领空在往跟到调用返回了）。

</blockquote>
下断后，点击“Check it Baby!“，按理来说我们应该断在 MessageBoxA 函数的段首，但是没，也没有弹出错误提示，整个程序也没有退出，检查了一下，也没有线程异常挂起等等。我感觉可能我们刚刚去 NAG 弹窗的时候 nop 掉的函数有问题，我立即吧源程序拖入 OD，正常走过弹窗后，重给 MessageBoxA 下断，程序能被断下，F9 继续走，程序正常弹出错误提示。
ok，看来我们去除弹窗的时候，把整个弹窗逻辑都会走的函数给 nop，那我们继续往回跟几层函数是层层调用的，内部函数走到 ret，就会回到上层调用），我发现有一个可以的位置：004563d，我们把它 nop 掉，保存为 Acid burn2,然后重复上述过程，ok=此时错误提示弹窗可正常被断下了。

后我们看下右下角堆栈窗口，调用来自“0042A1AE”,右键——> 反汇编窗口跟随

这个位置是不是跟熟悉，在上一节取出弹窗时候，直接给他干掉了，难怪后面断不下。我们继续一层，

来到下面这个位置，发现有错误提示，另一个应该就是正确提示了

ok，我们找到这段的段首，下断，F9 运行起来，在点一次“Check it Baby!“，程序果然停在这里，F8 单步往下走，不难发现，在 0042FB03 的位置就是关键跳，我们现在的目标破解即可，所以不要多说，直接 nop 掉这句。保存修改代码为 Acid burn3.exe，然后运行，输入伪，ok，爆破成功！
<blockquote>
这个过程中，我们会发现一些有趣的汇编代码，比如 livisun，l，v，i 像是在循环然后计算什么我们推测这边应该就是算法了，一会儿来研究下，然后写个注册机。
</blockquote>

<h2 id="3-破解另一个Serial">3.破解另一个 Serial</h2>
晚点，在来更新。。。