从这篇文章开始，我们要进入字节码实际应用的部分了。

因为字节码玩的炉火纯青，在工作休闲之余，「无痛」破解了一大波 Java 系软件。这里的「无痛」指的是不需要破坏原始 Jar 包或者 War 包，就可以达到破解目的

下面列举了一些折腾过的软件

- 分析 GC 日志的桌面端软件 censum (https://www.jclarity.com/censum/)
- 分析 GC 日志和线程的 gceasy和fastthread
- Intellij 上 Mybatis 插件（低版本），高版本使用了代码混淆，导致阅读比较困难，没有去折腾
- ELK 铂金版
- 供应商的 jar 包对指定 Mac 地址授权，切换服务器或者切换到 Docker 环境以后，就没办法使用

0x01 工欲善其事必先利其器

下面是常用的一些工具

- 字节码反编译查看工具 jdgui，luyten
- 字节码浏览工具 jclasslib
- ASM（后面会专门介绍）
- vim、hex editor

0x02 破解的几种方式

- 解包、直接修改 class 文件
  这种适用于非常简单，改动一些常量就可以完成的情况；
- 解包、通过 asm 工具修改 class 文件
  适用于逻辑较为复杂的情况；
- 通过-javaagent启动参数，动态修改（无痛破解）
  前面两种都属于破坏了原始的 class 文件，不属于「无痛破解」，如果要破解的软件升级了，需要重新修改打包，非常麻烦。采用 Java
  agent 的方式，只用在命令行启动参数里面加入一行参数就可以了。后续软件升级了，都不用修改 agent 的源码，非常方便，后面将会重点介绍这种方式。

0x03 第一个破解项目 censum

项目 censum jar 包地址放在了[github (https://github.com/arthur-zhang/geek01/blob/master/crack/censum-full.jar)](https://github.com/arthur-zhang/geek01/blob/master/crack/censum-full.jar) 上，使用jdgui打开，发现没有混淆，找到CensumStartupChecks类，里面是判断 license 是否合法、是否过期。下面代码做了一些精简。

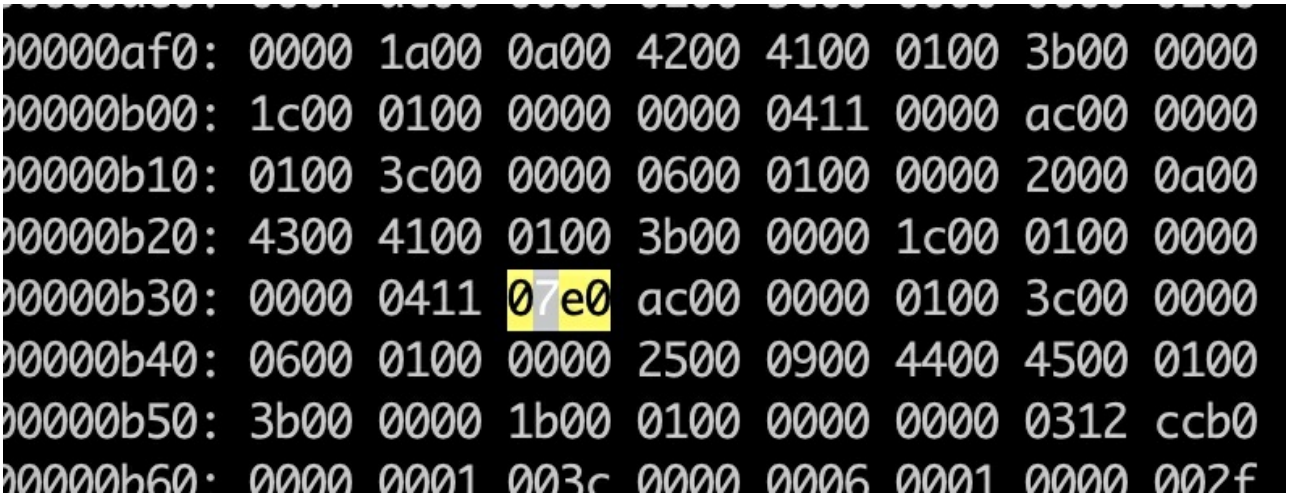
```
 public class CensumStartupChecks
{
  private static int getDayOfMonth() {
```

```
    return 7;
  }

  private static int getMonthOfYear() {
    return 0;
  }

  private static int getYear() {
    return 2016;
  }

  public static CanLoadState canLoadCensum()
  {
    validateLicensing();
    GregorianCalendar currentDate = new
GregorianCalendar();
    GregorianCalendar expiryDate =
getExiryDate();
    if (currentDate.after(expiryDate)) {
      return CanLoadState.LICENSE_EXPIRED;
    }
    return CanLoadState.SUCCESS;
  }

  public static GregorianCalendar getExiryDate()
  {
    return new GregorianCalendar(getYear(),
getMonthOfYear(), getDayOfMonth());
  }
}
```

可以看到，这个判断是否过期的方法很粗暴，直接拿当前时间与过期时间做对比，如果当前时间晚于过期时间，就返回 license 已过期。

要破解这个软件，一个最简单的思路就是把过期的年份2016修改一下，改为2226之类的。
我们知道 jar 包本质上就是一个 zip 压缩包，我们用 unzip 以后可以拿到所有的 class 文件

用 vim 打开vim -b ./com/jclarity/censum/CensumStartupChecks.class
使用 16 进制模式打开:%!xxd
搜索 2016 的十六进制(07e0)



使用vim命令修改成08a8(2216年)，回到普通模式:%!xxd -r保存退出

然后使用zip包打包zip -r ../censum-crack.jar . *

运行java -jar censum-crack.jar

可以看到，这种方式比较麻烦，我们会讲如何不修改源 class 文件的方法来无痛破解 Java 系软件，不过这之前，我们需要学习 ASM 和 javaagent 的原理

0x04 小结与思考题

这篇文章我们讲解了如何通过直接修改 class 文件的方式来破解软件，一起来回顾一下要点：

- 第一，破解软件常见有几种方式，修改 class 文件、javaagent 动态注入；
- 第二，jar 包其实是一个 zip 包，我们可以用标准的 zip、unzip 进行 jar 包的打包、解包。

留一道思考题，你平时遇到了哪些付费的 Java 系软件？你可以找到具体判断 license 是否合法的函数吗？有办法通过本文中介绍的方式破解吗？

欢迎你在留言区留言，和我一起讨论。