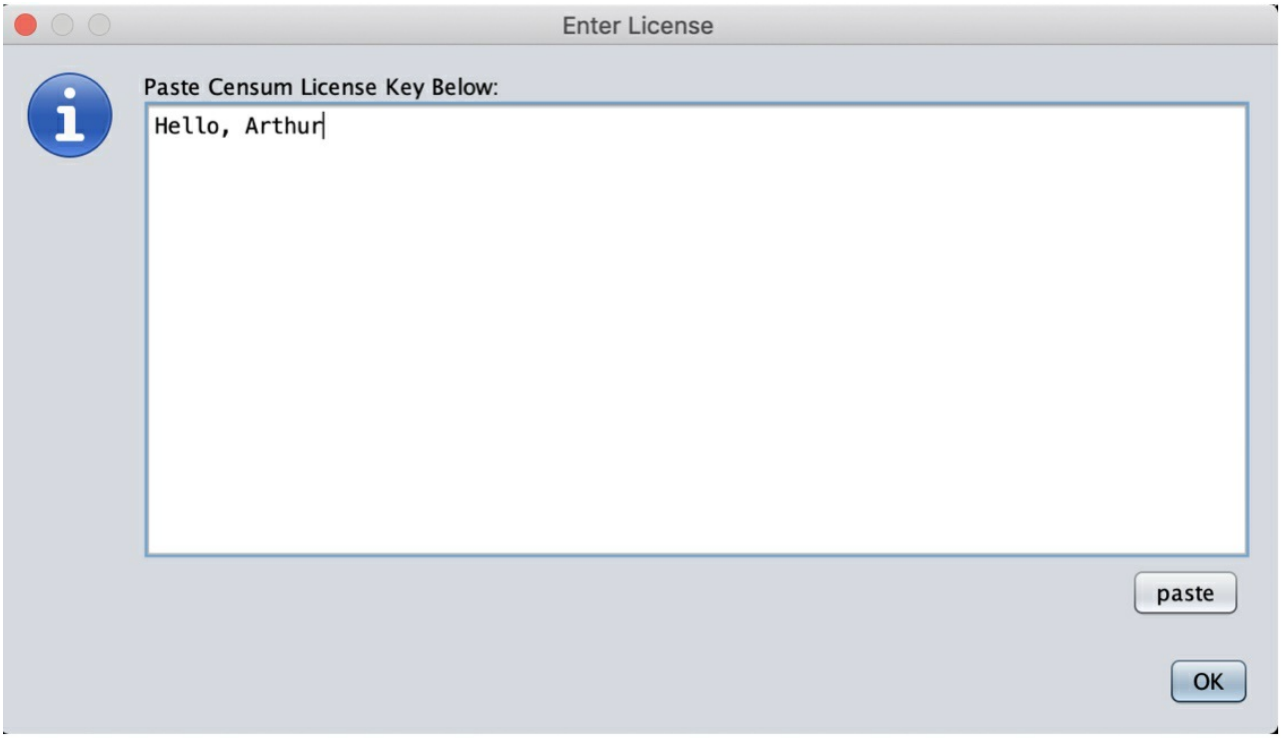
前几天热心的读者 xor eax，eax 反馈之前介绍过的破解方式已经不适用新版本的 censum 了，我花了一点时间找到了无痛破解的方法，下面是寻找破解过程中的一些思路，分享给大家，希望对你有所启发。

0x01 初体验

Mac 下的最新版 censum 是一个 dmg 包，真正的启动 jar 包在`/censum.app/Contents/Java/censum-full.jar`目录下。censum 新版本需要 jdk9 以上才可以运行。



0x02 找入口函数

有较多的方法可以找到整个 jar 的入口 main 函数，下面介绍两种方法

方法一：META-INF/MANIFEST.MF

jar 包的M ETA-INF/MANIFEST.MF 中保存了入口函数的信息，解压 jar 包就可以看到

```
Manifest-Version: 1.0
Created-By: jClarity
Build-Jdk: 9.0.1
Built-By: jClarity
Main-Class: com.jclarity.censum.Censum
censum-version: 5.0.4
```

方法二：查看类加载的方式

java 启动参数里面有一个-verbose:class选项，可以看到 JVM 运行时加载的类。比如执行java11 -verbose:class -jar censum-full.jar。由于类比较多，可以用 grep 命令过滤一下

同样可以看到第一个加载的 censum 库相关的类是 com.jclarity.censum.Censum

0x03 如何找到 license 校验相关的逻辑

按图索骥，按第一张图里面的提示，我们可以搜索这个字符串出自哪个 class 文件。

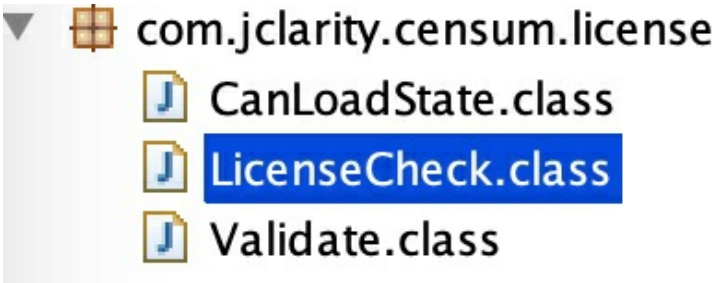
命令行进入 jar 包解压以后的文件夹：cd censum-full

搜索指定的字符串：grep -R "No license key" ., 找到了命中的 class 文件：Binary file ./com/jclarity/censum/license/CanLoadState.class matches

CanLoadState 是一个枚举类

```
public enum CanLoadState
{
    SUCCESS("Your license will expire after %1$te/%1$tb/%1$tY", "License Checked", true),
    LICENSE_EXPIRED("Your license has expired, please contact jClarity for a new license, support@jclarity.com", "License Expired", false),
    NO_LICENSE_PRESENT("No license key could be found, please contact jClarity for a new license, support@jclarity.com", "No License", false),
    LICENSE_SOON_TO_EXPIRE("Your license will expire soon.  Censum will not be usable after %1$te/%1$tb/%1$tY", "License Expiring Soon", true);
}
```

到此 license 相关性比较大的包和类就出来了



LicenseCheck 反编译以后的部分代码如下

```
public class LicenseCheck
```

```
{
    public LicenseCheck(final CanLoadState
canLoadState) {
        this.canLoadState = canLoadState;
        this.uuid = null;
        this.expireDate = null;
        this.email = null;
    }

    public LicenseCheck(final String props)
throws IOException {
        final Properties properties = new
Properties();
        properties.load(new
ByteArrayInputStream(props.getBytes(StandardChars
ets.UTF_8.name())));
        this.uuid =
properties.getProperty("license.uuid");
        this.email =
properties.getProperty("license.email");
        this.expireDate =
LocalDate.parse(properties.getProperty("license.e
xpiryDate"), DateTimeFormatter.ISO_LOCAL_DATE);
        if (this.expireDate == null) {
            this.canLoadState =
CanLoadState.NO_LICENSE_PRESENT;
        }
        else {
            final LocalDate now =
LocalDate.now();
            if (now.isAfter(this.expireDate)) {
                this.canLoadState =
CanLoadState.LICENSE_EXPIRED;
```

```
            }
            else if (now.plus(10L,
(TemporalUnit)ChronoUnit.DAYS).isAfter(this.expir
eDate)) {
                this.canLoadState =
CanLoadState.LICENSE_SOON_TO_EXPIRE;
            }
            else {
                this.canLoadState =
CanLoadState.SUCCESS;
            }
        }
    }
    public CanLoadState getCanLoadState() {
        return this.canLoadState;
    }
}
```

0x04 第一次破解尝试

第一个思路就是直接注入public CanLoadState getCanLoadState()，让它返回 CanLoadState.SUCCESS 就可以了

```
改造前
public CanLoadState getCanLoadState() {
    return this.canLoadState;
}
改造后
public CanLoadState getCanLoadState() {
    return CanLoadState.SUCCESS;
}
```

对应的字节码如下

```
getstatic
'com/jclarity/censum/license/CanLoadState.SUCCESS'
,'Lcom/jclarity/censum/license/CanLoadState;'
areturn
```

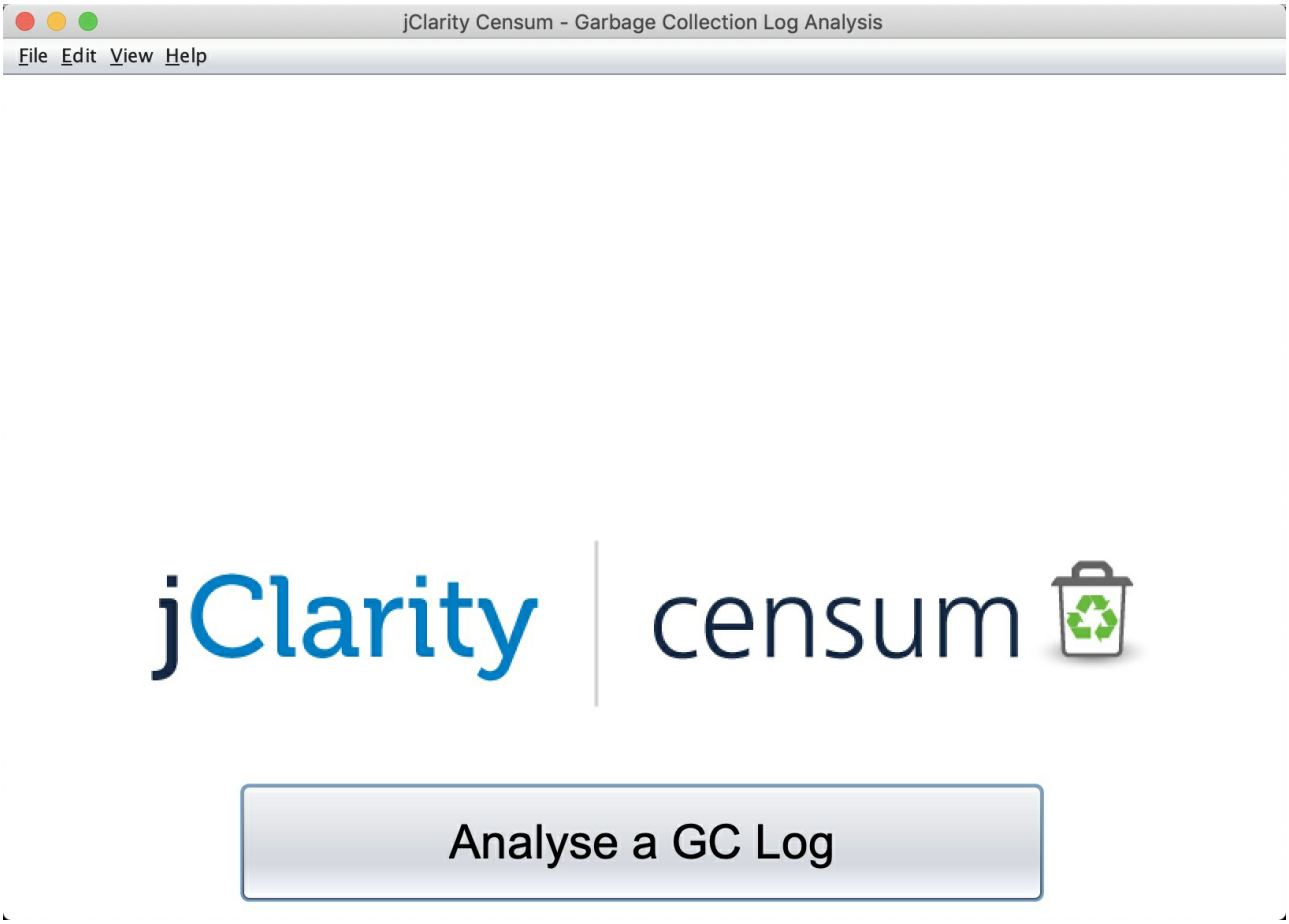
核心的 ASM 代码如下

```
public static class MyClassVisitor extends
ClassVisitor {
    private String className;
    @Override
    public MethodVisitor visitMethod(int access,
String name, String desc, String signature,
String[] exceptions) {
        System.out.println("visiting: " +
className + name);
        MethodVisitor mv =
super.visitMethod(access, name, desc, signature,
exceptions);
        // 只注入 getCanLoadState 函数
        if (name.equals("getCanLoadState")) {
            return new MyMethodVisitor(mv,
access, name, desc);
        }
        return mv;
    }
}

public static class MyMethodVisitor extends
AdviceAdapter {
    @Override
```

```
    protected void onMethodEnter() {
        // 让函数强行返回 CanLoadState.SUCCESS;
        mv.visitFieldInsn(GETSTATIC,
"com/jclarity/censum/license/CanLoadState",
"SUCCESS",
"Lcom/jclarity/censum/license/CanLoadState;");
        mv.visitInsn(ARETURN);
    }
}
```

打包成 javaagent 的 jar 包，运行`java11 -javaagent:/path/to/my-javaagent.jar -jar censum-full.jar`，大功告成。



完整的代码见文末

0x05 寻求更简单的办法

重新阅读入口类，其 license 处理逻辑都放在 checkLicense 函数中。

```
private void checkLicense() {
    LicenseCheck loadState;
    if (CensumProperties.isLicensingEnabled()) {
        loadState =
CensumStartupChecks.checkLicenseServer();
    } else {
        LicenseInput licenseInput = new
LicenseInput();
        loadState = licenseInput.doCheck();
    }

    CensumStartupChecks.startupTasks();
    String warningBody =
String.format(loadState.getCanLoadState().getBody
(), loadState.getExpireDate());
    switch(loadState.getCanLoadState()) {
    case LICENSE_EXPIRED:
        JOptionPane.showMessageDialog(this,
warningBody,
loadState.getCanLoadState().getTitle(), 0);
        System.exit(-1);
        break;
    case NO_LICENSE_PRESENT:
        JOptionPane.showMessageDialog(this,
warningBody,
loadState.getCanLoadState().getTitle(), 0);
        System.exit(-1);
```

```
        break;
    case LICENSE_SOON_TO_EXPIRE:
        JOptionPane.showMessageDialog(this,
warningBody,
loadState.getCanLoadState().getTitle(), 2);
    case SUCCESS:
    }
}
```

上面第一次破解尝试，其实改的就是 loadState.getCanLoadState() 的返回值，把本来返回 NO_LICENSE_PRESENT 的改为了 SUCCESS。那尝试一个更胆大的做法，能否直接跳过执行 checkLicense 函数，不用关注里面的具体的逻辑？也即改为

```
private void checkLicense() {
    return;
}
```

对应我们的 ASM 改写代码如下：

```
public static class MyClassVisitor extends
ClassVisitor {
    private String className;
    @Override
    public MethodVisitor visitMethod(int access,
String name, String desc, String signature,
String[] exceptions) {
        System.out.println("visiting: " +
className + name);
        MethodVisitor mv =
super.visitMethod(access, name, desc, signature,
exceptions);
        if (name.equals("checkLicense")) {
            return new MyMethodVisitor(mv,
access, name, desc);
        }
        return mv;
    }
}

public static class MyMethodVisitor extends
AdviceAdapter {
    @Override
    protected void onMethodEnter() {
        // 强行 return，不执行后面的 license 合法性检
查
        mv.visitInsn(RETURN);
    }
}
```

如上打包成 jar 包，用 javaagent 的方式启动 censum-full.jar，同样可以成功。

完整的代码我放在了 github 上：https://github.com/arthur-zhang/censum_new_version_crack

0x06 小结

这篇文章主要讲了如何破解最新版本 censum 软件。要点如下：

- 第一，可以通过解压 jar 包和 `java -verbose:class` 两种方式来找到入口 main 函数；
- 第二，如何通过 grep 命令找到 license 相关的代码；
- 第三，通过两种不同的方式使用 ASM 与 javaagent 来无痛破解。

0x07 思考

留一道作业题，你可以找到 Censum 其它的注入类和函数也实现同样破解的功能吗?

欢迎你在留言区留言，和我一起讨论。