【软件安全】Patch Cobalt Strike3.8 去除后门并修补功能

lz1y / 2018-03-16 11:49:51 / 浏览数 30953 技术文章 技术文章 顶(0) 踩(0)

---

Cobalt strike作为一款渗透测试工具，因其的钓鱼攻击体系的完备性，以及可简单的编写Aggressor-Script（Cobalt strike3）增强或增加其功能，所以在APT以及渗透中有很高的可用性。以下均称之为CS

之前就已经有人分享过Cobalt Strike 3.8破解版
但是经过笔者的一段时间使用后，发现试用版还存在许多的问题。
已知问题：

1. 由于网上绝大多数的CS3.8都是直接修改了试用日期，所以导致很多试用的"后门"都仍然存在。如图就是添加进去的指纹，因此CS通信会被很多IDS拦截请求。
2. 同类通道只能开一个端口

所以我们先直接将CS改成正式版本的，就可以简单快捷的解决很多未知问题了。
我是windows平台，所以选择JD-GUI来反编译CS，CS并没有混淆，众所周知...java和python类似，都是先编译成字节码然后执行的，这也是它们可以跨平台的原因，但是
CS结构：

问题一既然是判断是否为正式版，我们根据方法名 "License.isTrial"，搜索到方法所在common.License.isTrial()
返回值为布尔类型，所以我们只需要将其返回值修改为True，即可摇身一变，变为正式版本了。

修改方案有两种，一个是使用javassist直接修改字节码，还有一个方法就是利用JAD反编译为JAVA文件，然后javac重新编译为class文件。
我这里使用第二种方案。
首先将cobaltstrike.jar以压缩包格式打开，复制License.class出来，然后运行"jad.exe E:\cobaltstrike3\cobaltstrike\License.class"
随即，"E:\cobaltstrike3\cobaltstrike\"目录下就会生成License.jad，修改后缀为java，即是源码文件了。

修改返回值为TRUE。
保存，运行"javac -classpath cobaltstrike.jar License.java"
然后同目录会覆盖生成License.class，直接复制License.class，替换cobaltstrike.jar中的License.class即可成功修改。
直接将isTrial函数patch会有一个弊端，那就是试用版本缺少一个XOR.BIN文件，没有办法对payload编码。所以，得去把编码步骤略过。函数名为"encode"自行搜索，按照

同理，修补同通道监听多个端口的功能也类似以上步骤，在此不累述了。直接搜索字符串修改代码即可。

单CS.jar:
需要替换服务端和客户端的JAR文件
链接: https://pan.baidu.com/s/1WT-UDr_O-1nUiT-Ch9PSMg 密码: x26t

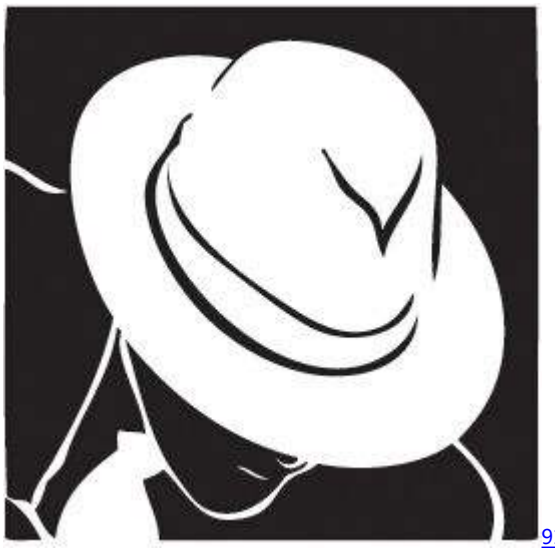
成品一套：
链接：https://pan.baidu.com/s/1dQoVbK 密码：jh1x

解压密码：Va1n3R!@#

Blog: http://www.lz1y.cn


上一篇：深入探索数据库攻击技术 Part 2 下一篇：利用暴力攻击破解登陆密码

1. 5 条回复



91shell 2018-03-16 19:26:29

谢谢分享，楼主有没有最新版的

0 回复Ta

---


lz1y 2018-03-17 00:39:58

@91shell 我也想有，都已经更新很多版本了，官方对于新版的管控特别严格。

0 回复Ta

---


xsser233 2018-11-03 19:06:35

反编译文末给的成品 发现License类的返回值为False，没改啊？？？

0 回复Ta

---


lz1y 2018-12-01 13:55:25

@xsser233 文中笔误了，实际成品是对的

0 回复Ta

---

xxxxxx 2018-12-02 10:23:31

@lz1y 师傅可以分享下3.12吗 github的全部被删了

0 回复Ta

---

登录 后跟帖

先知社区

---

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板