Enul1ttle

发表于 17 分钟前 打印 字体大小: 倒序看帖 跳转到 » 1 #

新手上路

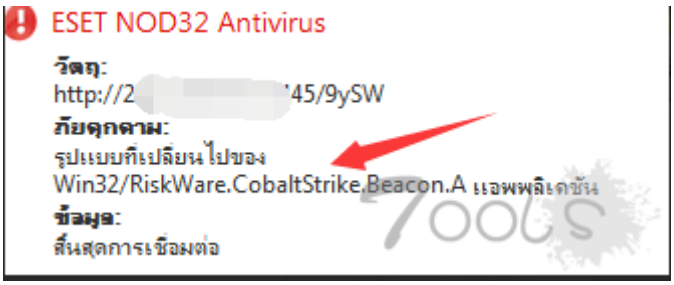
帖子 0
积分 0
TCV 0
TuBi 0
坛龄 0天

所需阅读权限 20

[【原创】] **投稿文章：Bypass ESET NOD32 HIPS**

前言

最近在渗透的过程中，发现木马在与C2通信的时候被ESET NOD Antivirus 的主机入侵预防系统（HIPS）给拦截了下来。并标识为 win32/RiskWare.CobaltStrike.Beacon.A。查了网上的资料，配置下 Malleable C2 Profiles 将其绕过。



0x01 生成新的ssl.store

在cobalt strike.jar里的/cloudstrike/NanoHTTPD.java 可以看到木马与C2通信默认使用的是resources/ssl.store，密码为123456。这是非常不安全的。所以我们首先重新生成新的ssl.store文件。

```
public SSLServerSocketFactory getSSLFactory(InputStream ksIs, String password)
{
    try
    {
        if(ksIs == null)
        {
            ksIs = getClass().getClassLoader().getResourceAsStream("resources/ssl.store");
            password = "123456";
```

- 生成新的ssl.store

```
keytool -keystore ssl.store -storepass password@t00ls -keypass password@t00ls -genkey -keyalg RSA -alias cs -dname "CN=it, OU=it, O=it, L=it, S=it, C=it"
```

- 迁移到行业标准格式 PKCS12

```
keytool -importkeystore -srckeystore ssl.store -destkeystore ssl.store -deststoretype pkcs12
```

0x02 编写Malleable C2配置文件

自己写太麻烦，我们用github上的项目进行修改:https://github.com/bluscreenofjeff/MalleableC2Profiles

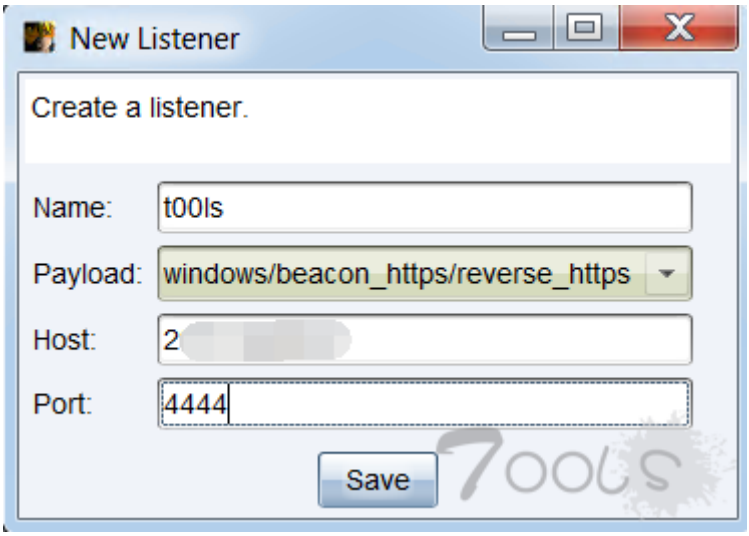
这里我用的是wikipedia_getonly.profile，把该文件放在与ssl.store同目录下。然后只需修改https-certificate{}里的内容。

```
#set https cert info
https-certificate {
      set keystore "ssl.store";
      set password "password@t00ls";
}
```

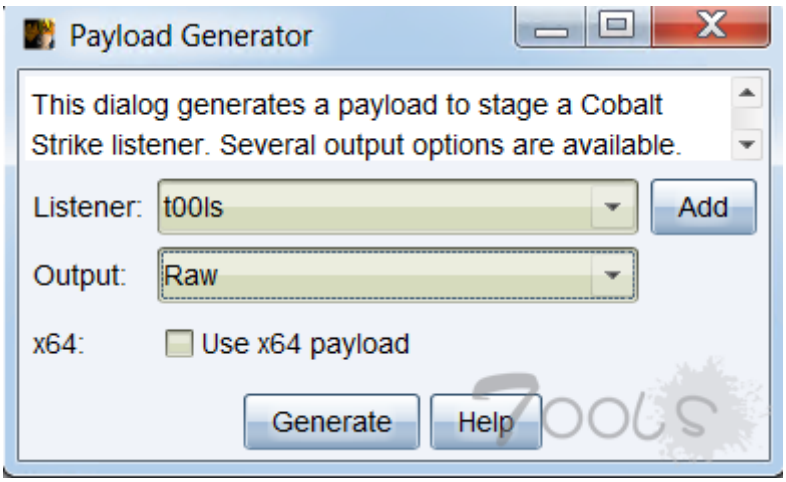
使用方式./teamserver {IP} {password} /root/MalleableC2Profiles/wikipedia_getonly.profile

0x03 shellter 捆绑cobalt strike payload 免杀

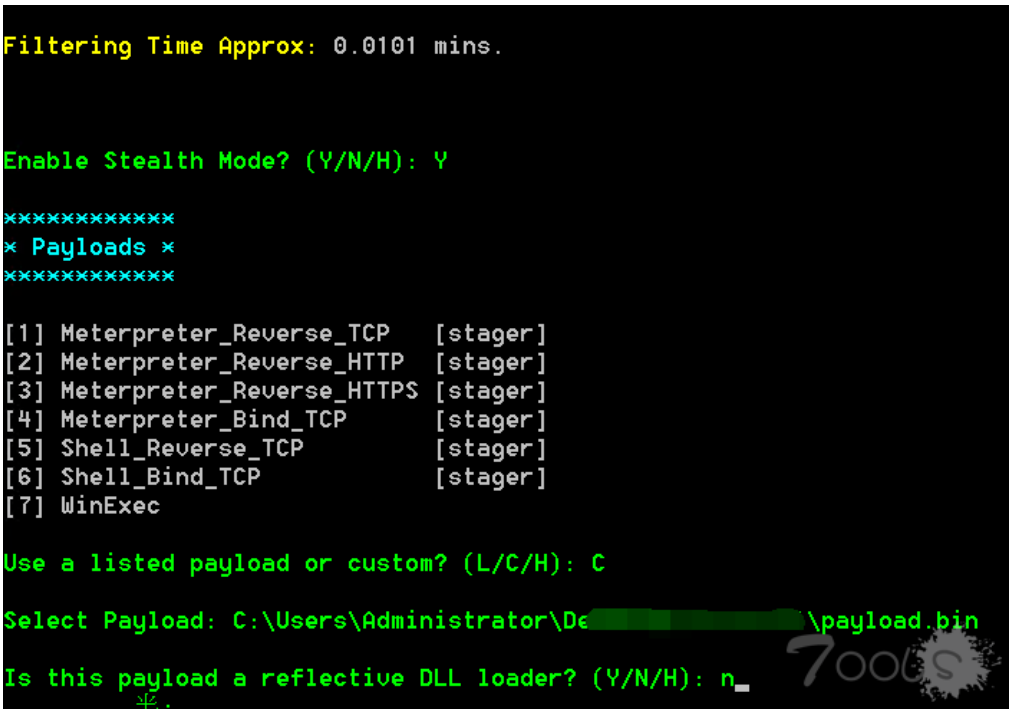
- 新建Listenner , Payload选择 windows/beacon_https/reverse_https



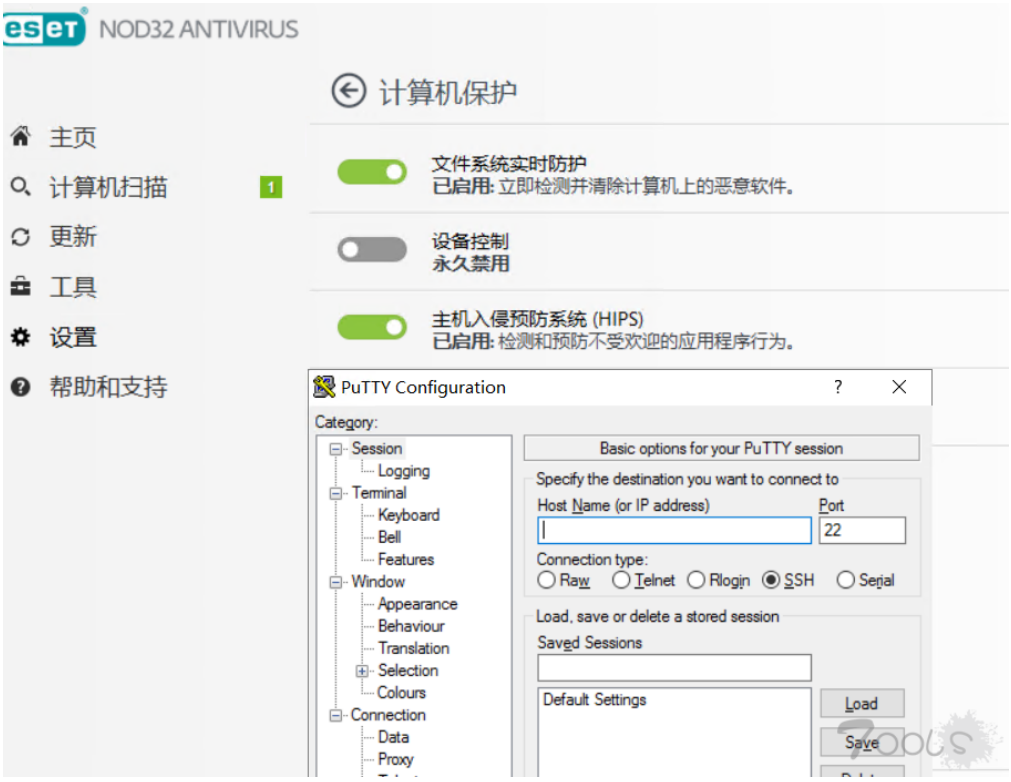
- 生成Payload :Attacks->Packages->Payload Generator->Output选择Raw->得到payload.bin

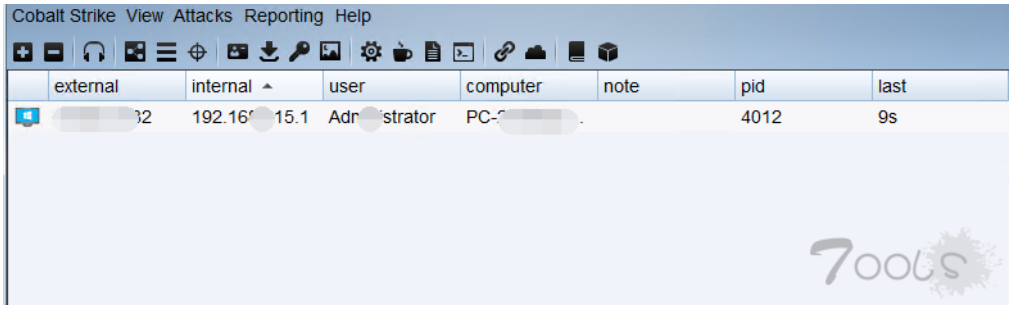


- 捆绑到putty.exe（只能是32位不加壳的exe)



0x04 免杀效果





0 0

顶 踩

0 0

打赏 拍砖 收藏 分享 支持 反对

回复 引用 编辑 使用道具

返回列表

高级模式

发表回复 回帖后跳转到最后一页