象 0x01 简介:

CuiRi 是一款红队专用免杀木马生成器,该工具可以通过红队人员提供的一段 shellcode 快速生成一个绕过所有杀软的可执行木马。

特点

- 1.基于 Syscall 进行免杀,且随机混淆,可过几乎所有杀软
- 2.内置 go-strip 对 Go 生成的木马进行编译信息抹除与程序信息混淆
- 3.工具本体只有 1 个 exe,搭配 Go 环境即可直接使用

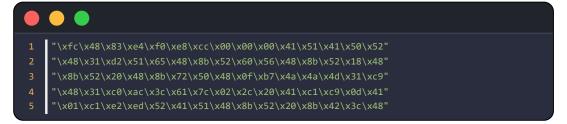
感谢 go-strip 作者 @boy-hack

从 <u>release</u> 中下载二进制文件,并且在系统上安装 Go 语言环境,然后将 shellcode 保存到1个txt文件中,即可使用本工具生成免杀马。



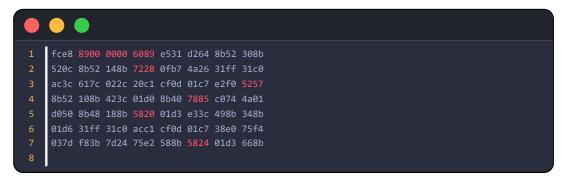
CuiRi 支持的 shellcode 格式分为以下两种:

1.C语言字符串格式 shellcode:



2.纯十六进制数值格式 shellcode:

注意: 如果是从 Cobalt Strike 中生成的 bin 文件,请单独将 bin 里的十六进制复制保存到一个 txt 文件中。



https://mp.weixin.qq.com/s/m4I_YDn98K_A2yGAhv67Gg

https://wiki.wgpsec.org/knowledge/hw/2020-defend-tips.html