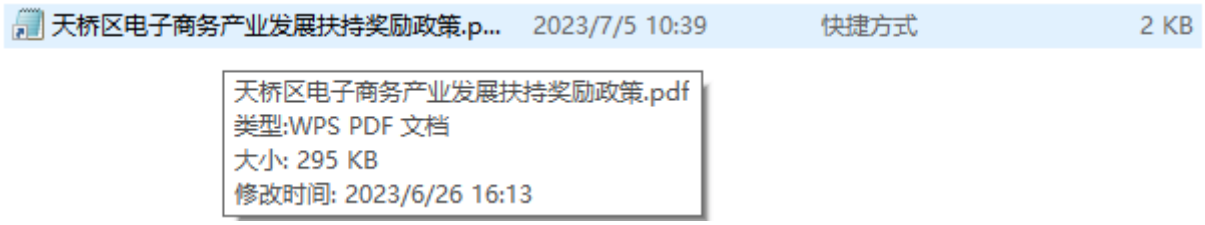
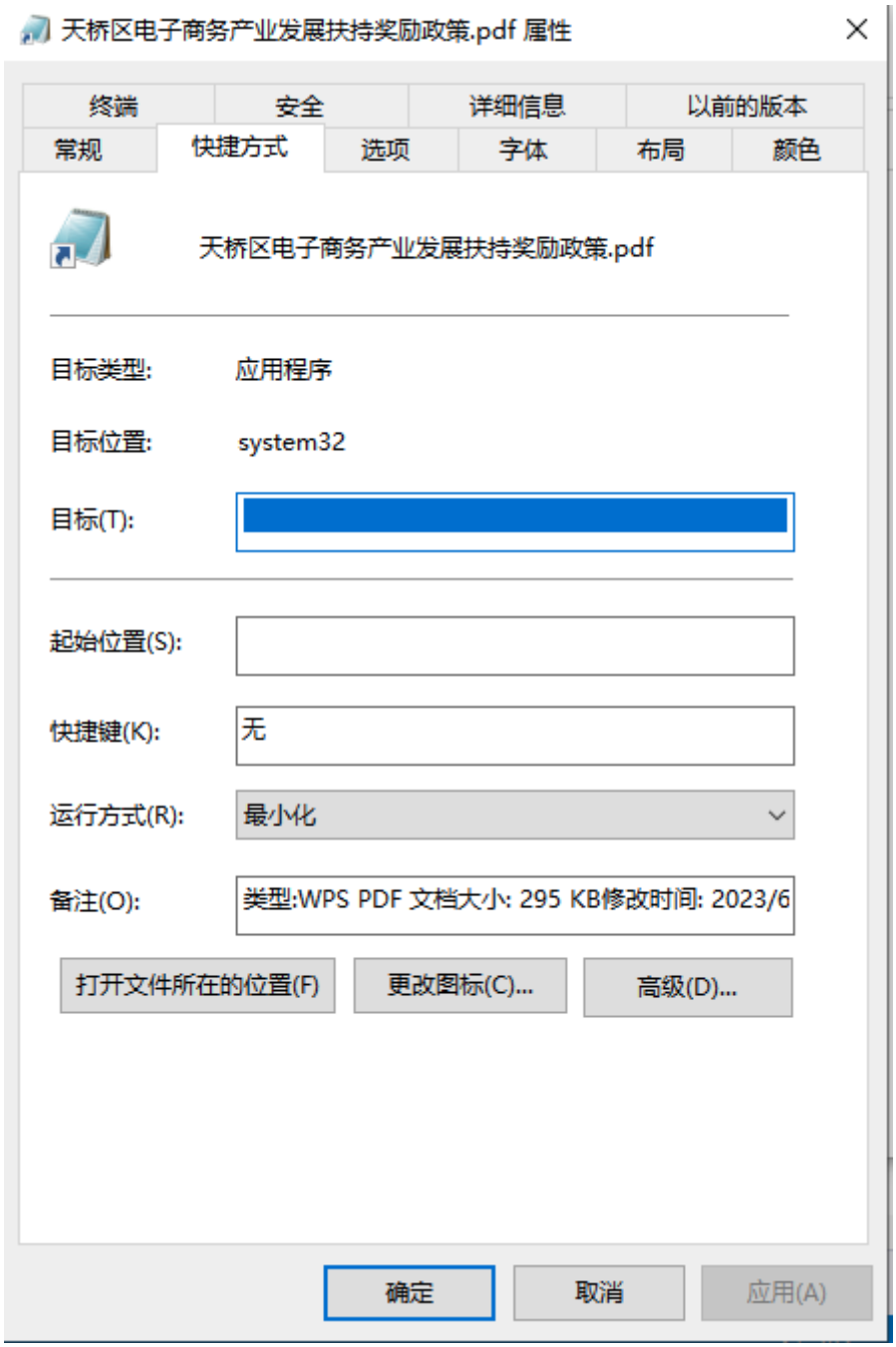
快捷方式生成

使用方法：

```
linkgen.exe test.pdf.lnk "类型:WPS PDF 文档\n大小: 295 KB\n修改时间: 2023/6/26 16:13"
```

然后会生成一个设置为好路径的快捷方式，通过cmd调用bat脚本

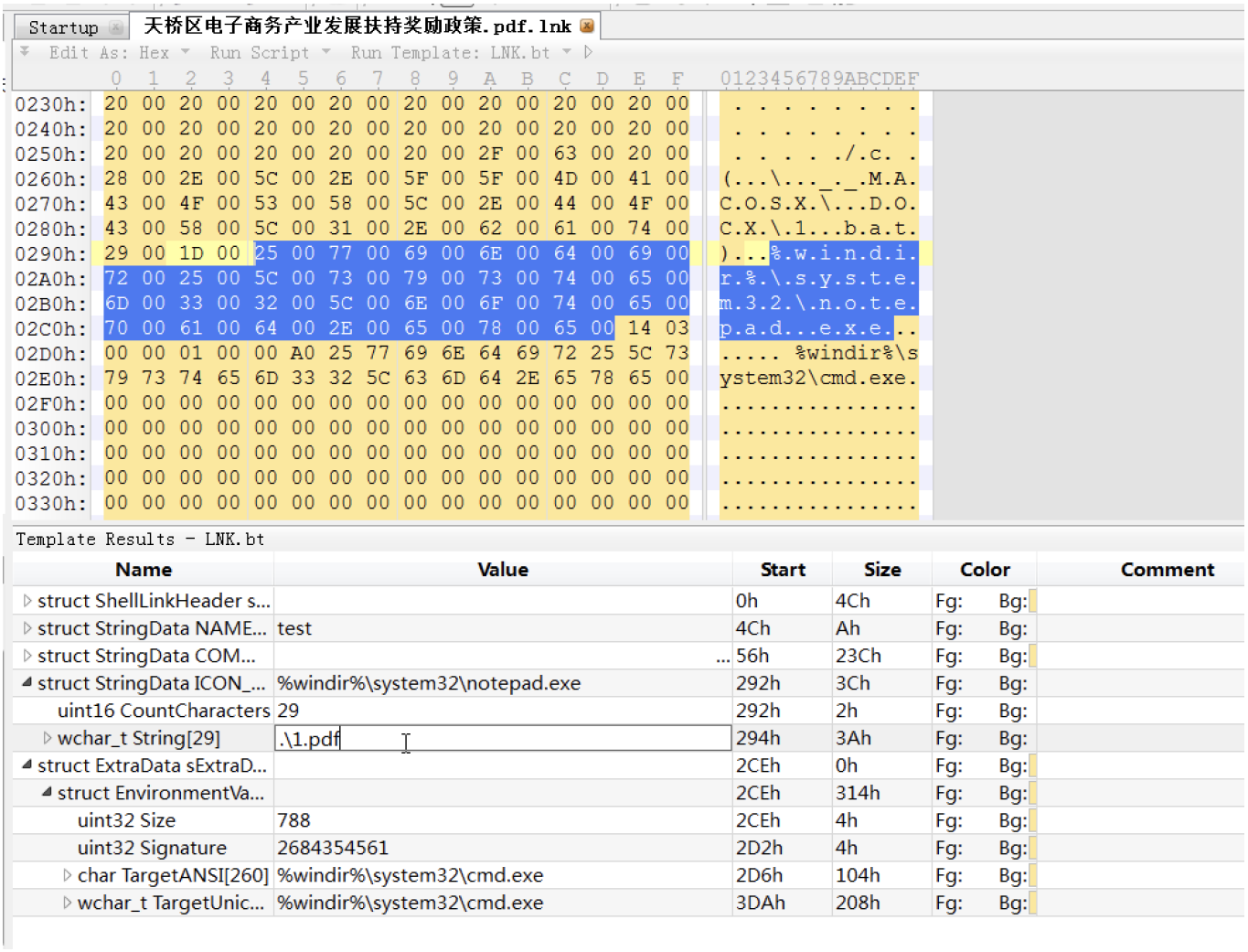




可以看到目标处填充了大量空格，而在目标处的字符长度是有限制的，我们后面的命令都会无法显示出来。

图标修改

通过010editor去修改快捷方式图标 将其图标出改为 .\1.pdf 可以在用户电脑中映射成对应的图标，原理和当你打开一个txt的后缀时系统会默认通过notepad.exe打开一样，都是通过注册表表项相关进行映射。

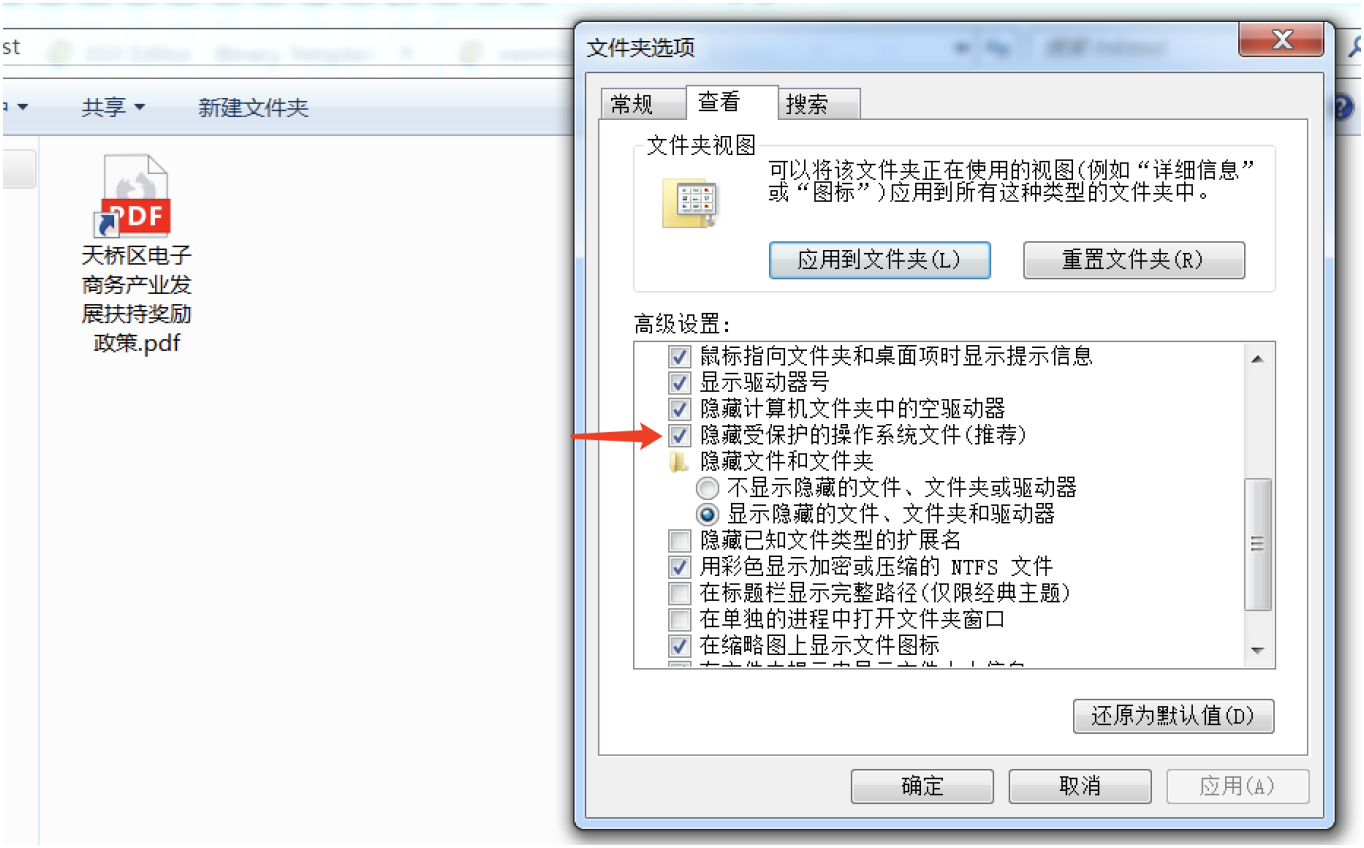


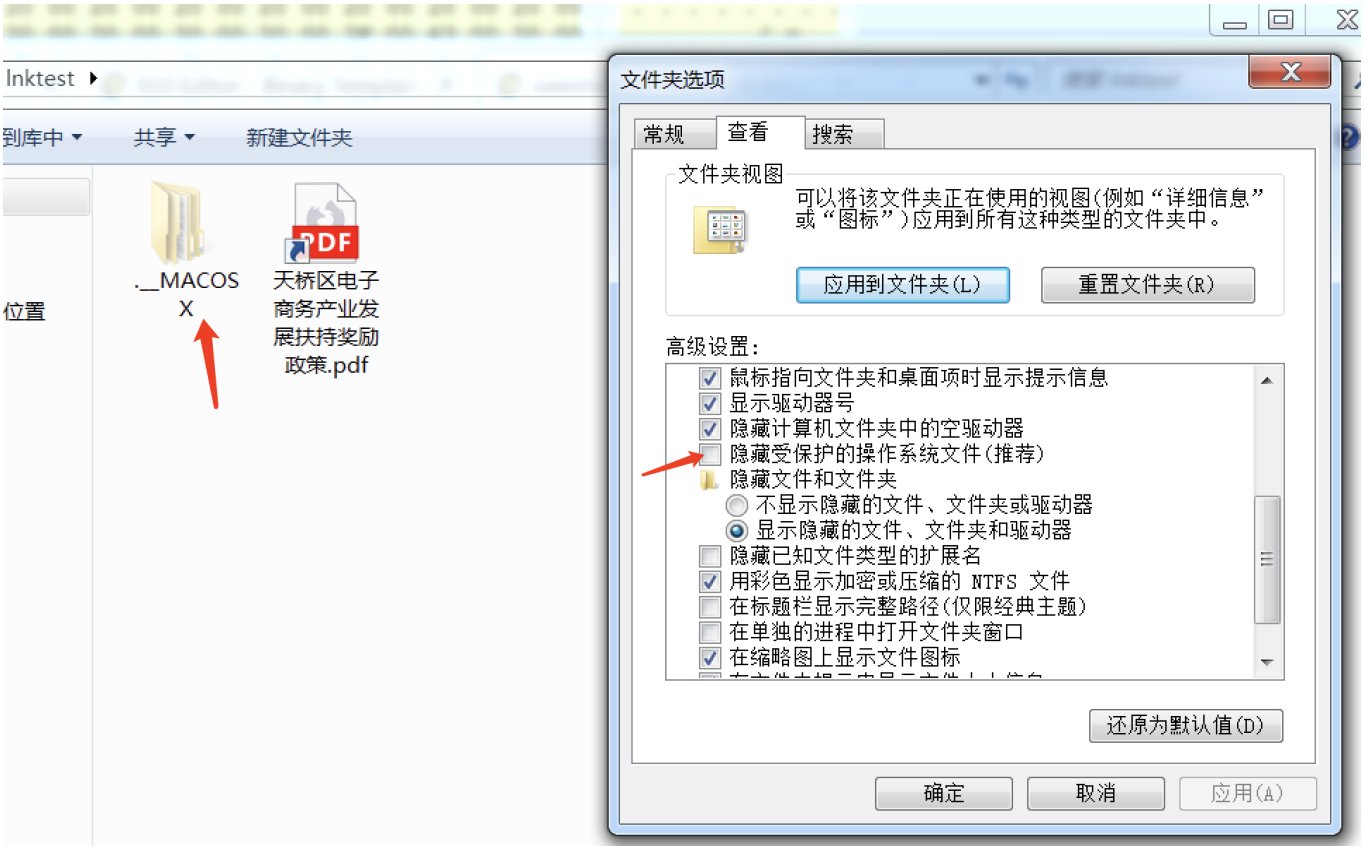
目录设置及利用原理

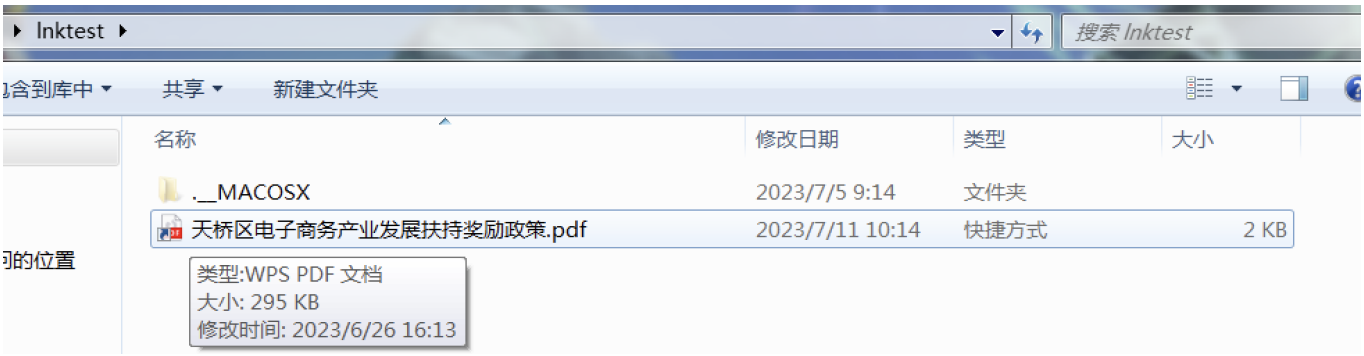
这里默认路径为 `.__MACOSX\.DOCX\1.bat`

由于考虑到在macos下的文件传到Windows系统下都会存在`.__MACOSX`所以就通过这个进行伪装

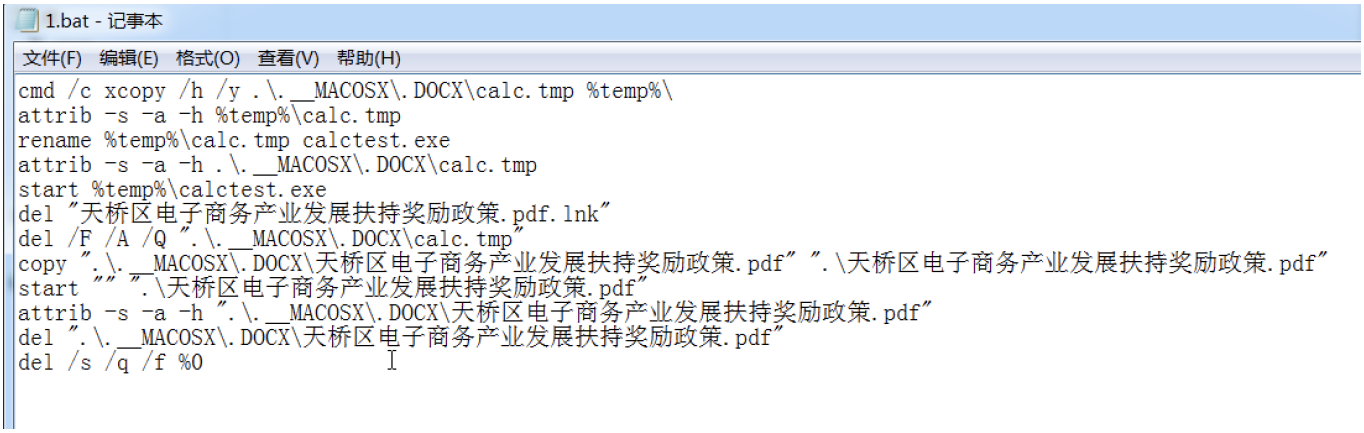
通过`attrib +s +a +h .__MACOSX`对存放木马文件和脚本及正常pdf的目录进行隐藏，正常情况下隐藏后将无法显示出来。


共享
新建文件夹
天桥区电子商务产业发展扶持奖励政策.pdf
文件夹选项
常规
查看
搜索
文件夹视图
可以将该文件夹正在使用的视图(例如“详细信息”或“图标”)应用到所有这种类型的文件夹中。
应用到文件夹(L)
重置文件夹(R)
高级设置:
鼠标指向文件夹和桌面项时显示提示信息
显示驱动器号
隐藏计算机文件夹中的空驱动器
隐藏受保护的操作系统文件(推荐)
隐藏文件和文件夹
不显示隐藏的文件、文件夹或驱动器
显示隐藏的文件、文件夹和驱动器
隐藏已知文件类型的扩展名
用彩色显示加密或压缩的 NTFS 文件
在标题栏显示完整路径(仅限经典主题)
在单独的进程中打开文件夹窗口
在缩略图上显示文件图标
还原为默认值(D)
确定
取消
应用(A)


lnktest
到库中
共享
新建文件夹
位置
.__MACOSX
天桥区电子商务产业发展扶持奖励政策.pdf
文件夹选项
常规
查看
搜索
文件夹视图
可以将该文件夹正在使用的视图(例如“详细信息”或“图标”)应用到所有这种类型的文件夹中。
应用到文件夹(L)
重置文件夹(R)
高级设置:
鼠标指向文件夹和桌面项时显示提示信息
显示驱动器号
隐藏计算机文件夹中的空驱动器
隐藏受保护的操作系统文件(推荐)
隐藏文件和文件夹
不显示隐藏的文件、文件夹或驱动器
显示隐藏的文件、文件夹和驱动器
隐藏已知文件类型的扩展名
用彩色显示加密或压缩的 NTFS 文件
在标题栏显示完整路径(仅限经典主题)
在单独的进程中打开文件夹窗口
在缩略图上显示文件图标
还原为默认值(D)
确定
取消
应用(A)

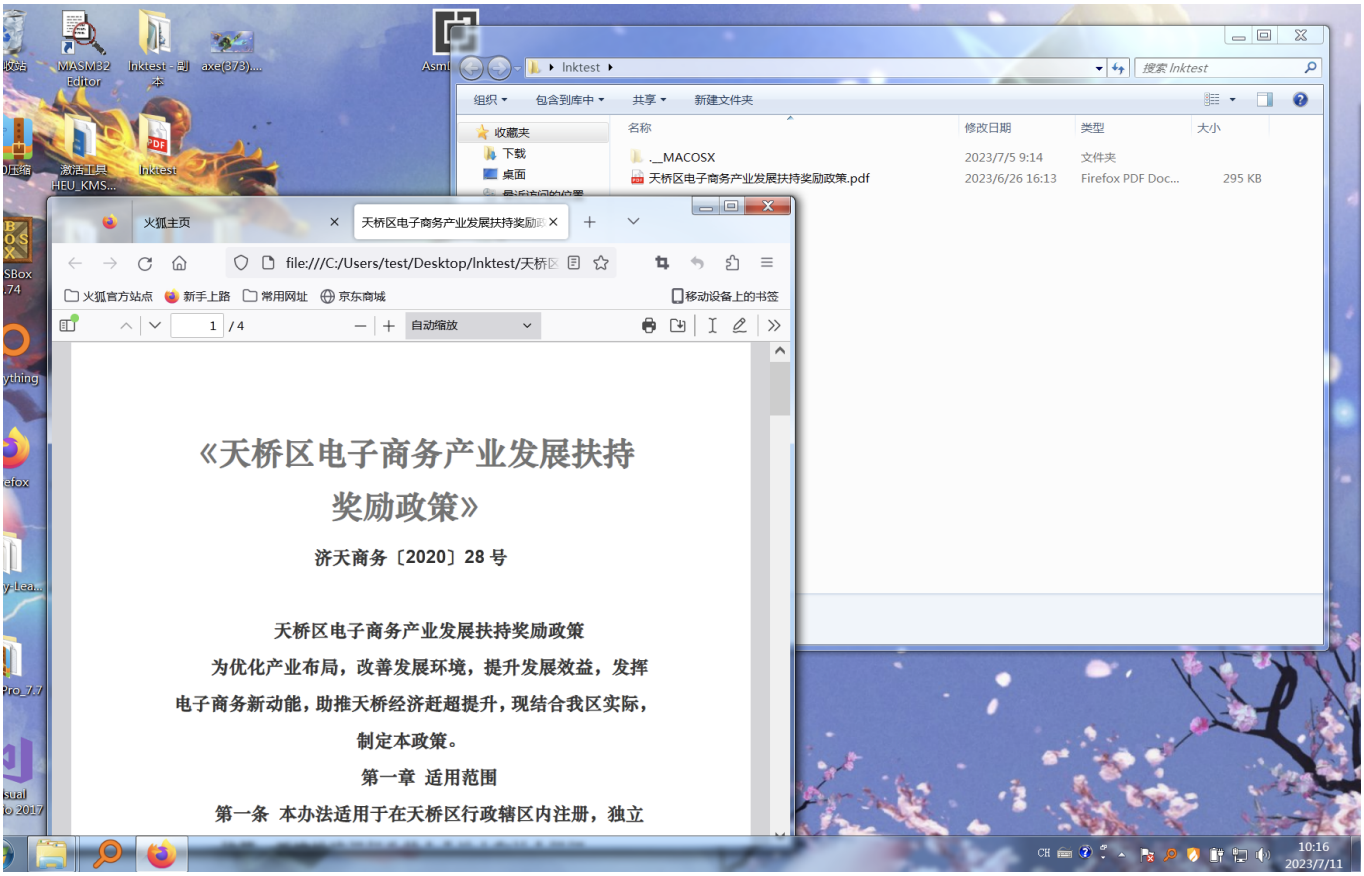


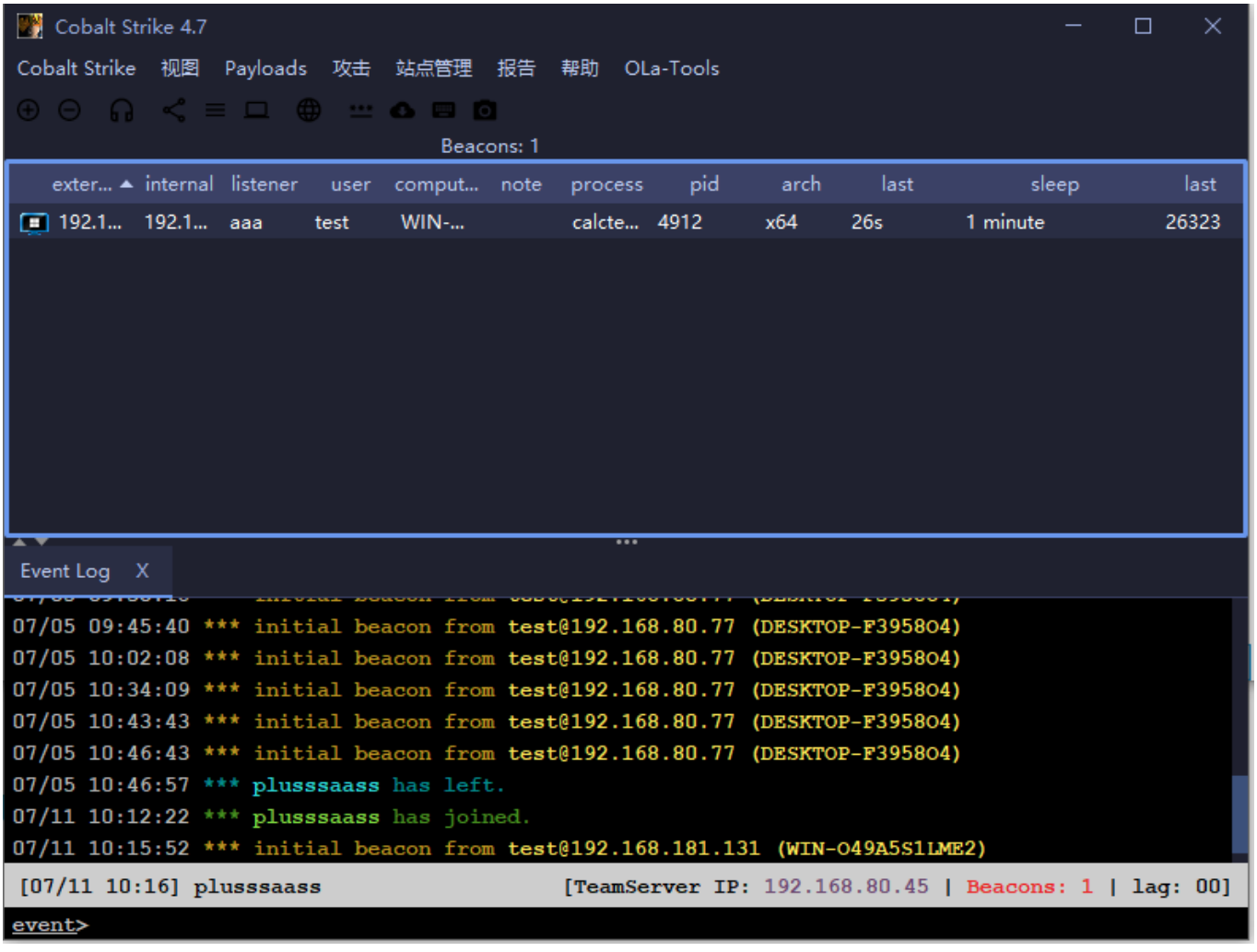
当用户点击快捷方式时就会运行bat脚本，将木马文件复制到其他目录下并改名运行，通过将bat脚本路径下的pdf正常文件替换到原快捷方式处「相同文件名」，并删除bat目录下的所有文件，实现通过lnk快捷方式+bat脚本的方式进行钓鱼，与该方法相同的还有通过wscript.exe调用vbs脚本 原理也差不多。



实际效果

当双击lnk快捷方式后 大约2s后会打开pdf文件并上线到CS


Inktest
组织
包含到库中
共享
新建文件夹
名称
修改日期
类型
大小
收藏夹
下载
桌面
._MACOSX
2023/7/5 9:14
文件夹
天桥区电子商务产业发展扶持奖励政策.pdf
2023/6/26 16:13
Firefox PDF Doc...
295 KB
火狐主页
天桥区电子商务产业发展扶持奖励政策
file:///C:/Users/test/Desktop/Inktest/天桥区
火狐官方站点
新手上路
常用网址
京东商城
移动设备上的书签
1 / 4
自动缩放
《天桥区电子商务产业发展扶持奖励政策》
济天商务〔2020〕28号
天桥区电子商务产业发展扶持奖励政策
为优化产业布局，改善发展环境，提升发展效益，发挥电子商务新动能，助推天桥经济赶超提升，现结合我区实际，制定本政策。
第一章 适用范围
第一条 本办法适用于在天桥区行政辖区内注册，独立
10:16
2023/7/11


Cobalt Strike 4.7
Cobalt Strike
视图
Payloads
攻击
站点管理
报告
帮助
OLa-Tools
Beacons: 1
exter...
internal
listener
user
comput...
note
process
pid
arch
last
sleep
last
192.1...
192.1...
aaa
test
WIN-...
calcte...
4912
x64
26s
1 minute
26323
Event Log
X
07/05 09:45:40 *** initial beacon from test@192.168.80.77 (DESKTOP-F395804)
07/05 10:02:08 *** initial beacon from test@192.168.80.77 (DESKTOP-F395804)
07/05 10:34:09 *** initial beacon from test@192.168.80.77 (DESKTOP-F395804)
07/05 10:43:43 *** initial beacon from test@192.168.80.77 (DESKTOP-F395804)
07/05 10:46:43 *** initial beacon from test@192.168.80.77 (DESKTOP-F395804)
07/05 10:46:57 *** plusssaass has left.
07/11 10:12:22 *** plusssaass has joined.
07/11 10:15:52 *** initial beacon from test@192.168.181.131 (WIN-O49A5S1LME2)
[07/11 10:16] plusssaass
[TeamServer IP: 192.168.80.45 | Beacons: 1 | lag: 00]
event>

「默认情况下是看不到`.__MACOSX`文件夹的」

不足

360会对自解压、lnk钓鱼等进行较为严格的把控，所以在一些360的机器上大概率无法成功