

Lnk 是现在主流钓鱼手法，一般实战中用的比较多的是用 lnk 伪装成 pdf，然后 pe 文件落地进行钓鱼。

缺点是有 pe 文件落地，优点是稳定。

当然，lnk 还可以进行远程加载，实战中约束较多，个人不太推荐。

这里先演示：

首先准备一个压缩包



解压出来得到一份文件：



打开查看：

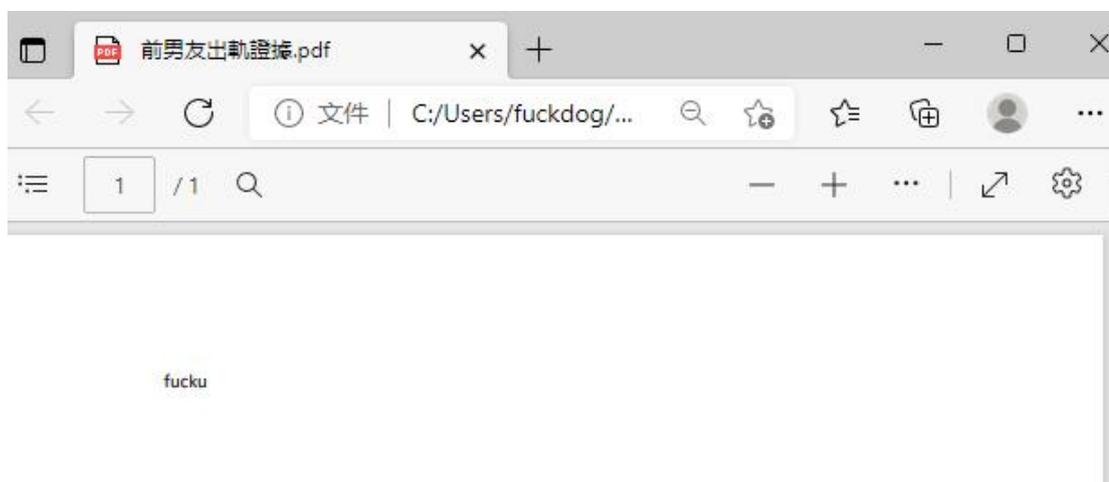


然后点击：

cs 这边已经成功上线

```
04/26 17:12:18 *** initial beacon from fuckdog@192.168.153.129
```

同时客户端会打开一份 pdf 文件，文案可以自己构造



最后这个文件就还是 pdf



怎么玩，很简单，其实网上有现成的代码可以复用
这里可以用 Yihsiwei 师傅的

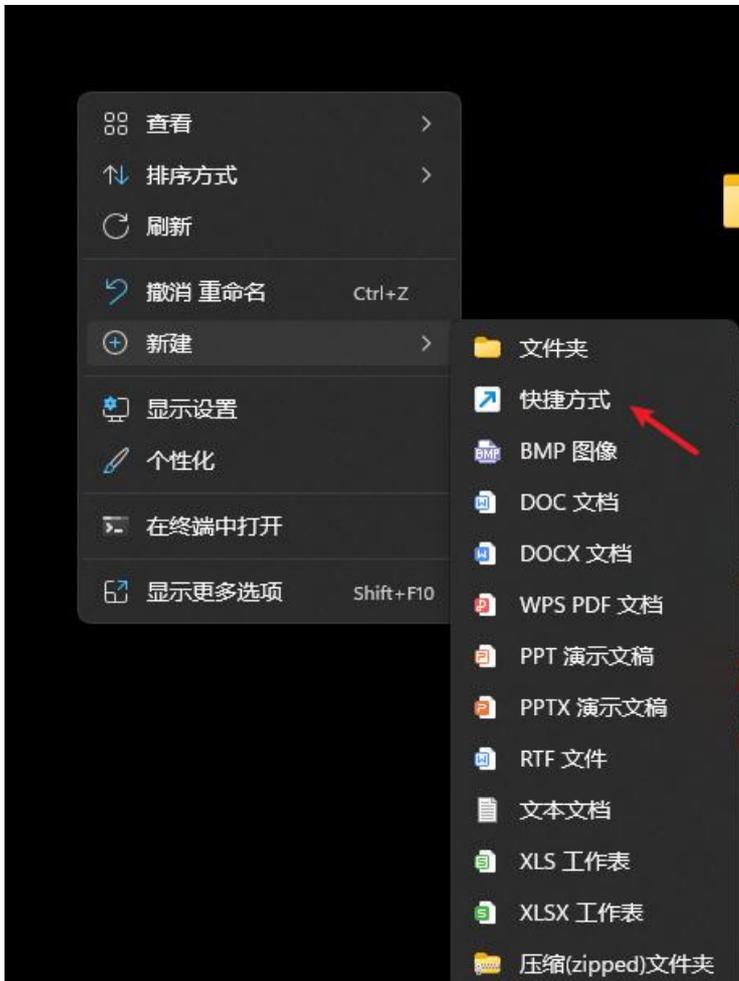
[//https://github.com/Yihsiwei/Lnk-Trojan](https://github.com/Yihsiwei/Lnk-Trojan)

使用方法在他的 github 下面也有，这里不多赘述

这里补充两个新的东西

1、如何将 lnk 变成 pdf 图标

普通我们创建 lnk 都是这样：



然后这里先随便填

← 创建快捷方式

想为哪个对象创建快捷方式?

该向导帮助你创建本地或网络程序、文件、文件夹、计算机或 Internet 地址的快捷方式。

请键入对象的位置(T):

calc.exe

浏览(R)...

单击“下一步”继续。

下一页(N)

取消

再命名

← 创建快捷方式

想将快捷方式命名为什么?

键入该快捷方式的名称(T):

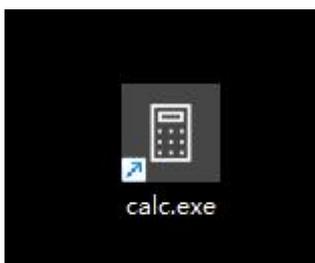
calc.exe

单击“完成”创建快捷方式。

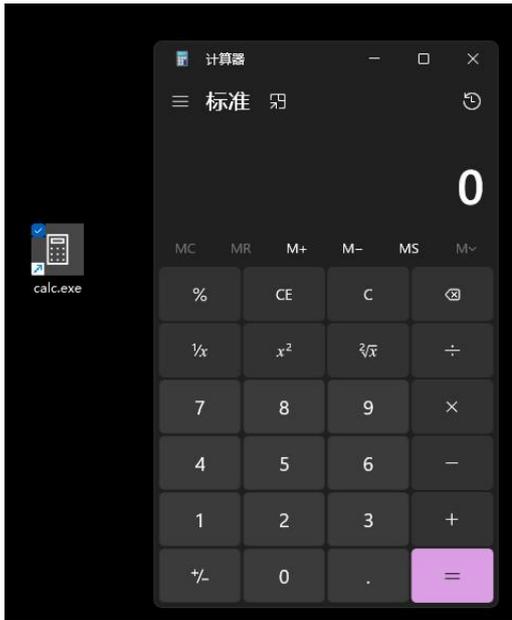
完成(F)

取消

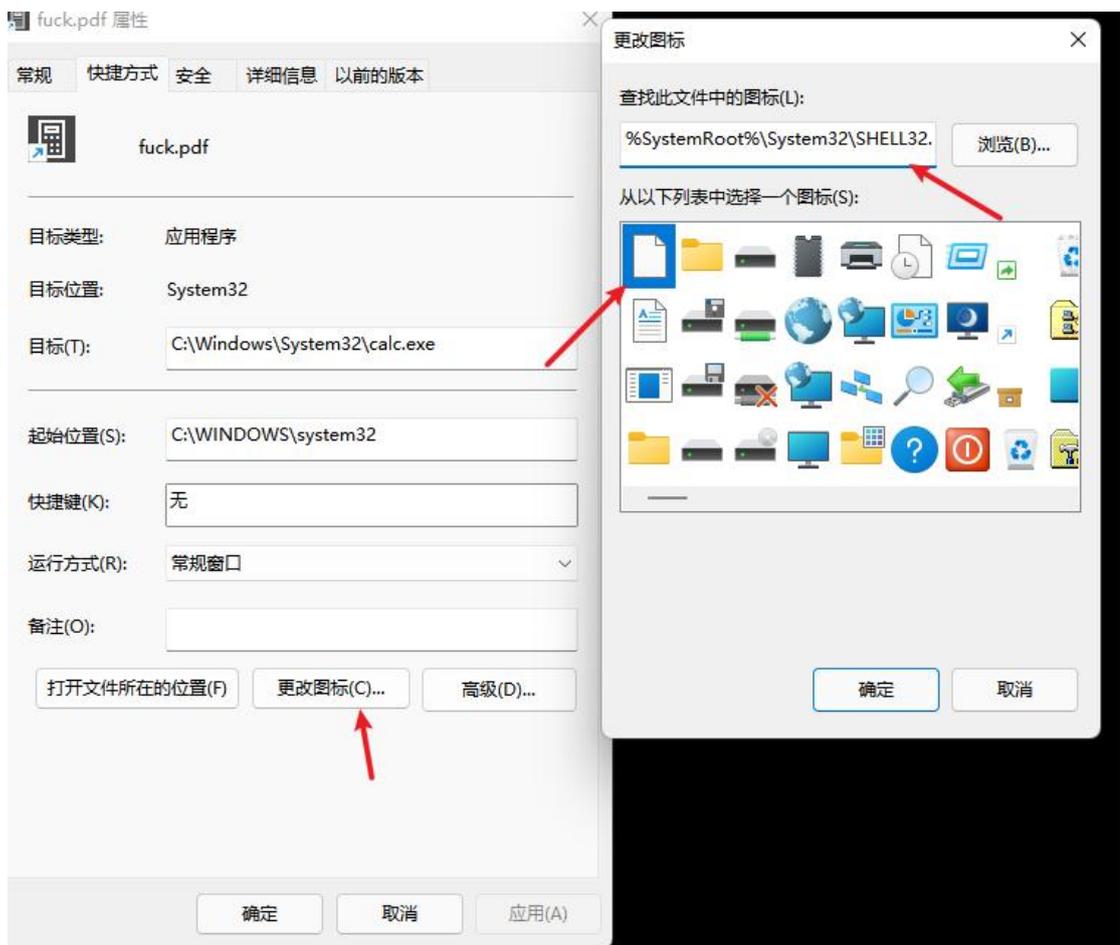
然后完成，就得到了一个 lnk 文件



双击运行，发现会调用计算器，因为我填写的 src 就是计算器



这里进行图标修改



然后重命名，就得到了一份初始的 Ink。



但是这里图标并不是 pdf，怎么办呢？

这里需要用 010editor 进行修改文件数据

导入文件，然后 Ctrl+f 搜索 6C00

模板结果 - LNK.bt

名称	值	开始	大小	颜色	注释
> struct ShellLinkHeader sShellLi...		0h	4Ch	Fg: Bg:	
> struct LinkTargetDList sLinkTa...	CLSID_MyComput...	4Ch	13Bh	Fg: Bg:	
> struct LinkInfo sLinkInfo		187h	51h	Fg: Bg:	
> struct StringData RELATIVE_PA...	..\..\Windows\Sy...	1D8h	46h	Fg: Bg:	
> struct StringData WORKING_DIR	C:\WINDOWS\sys...	21Eh	28h	Fg: Bg:	
> struct StringData ICON_LOCAT...	%SystemRoot%\S...	246h	44h	Fg: Bg:	
> struct ExtraData sExtraData		28Ah	2C1h	Fg: Bg:	

查找结果

地址	值
212h	6c00
286h	6c00
288h	6c00

搜索完毕之后，替换 icon 的地址为.\1.pdf

注意这里需要使用 unicode 编码

行号

可转码

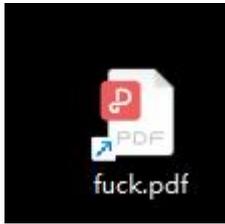
- 使用默认(D) '十六进制(H)' 字符集
- ASCII - ANSI(A)
- Unicode(U)
- UTF-8(B)
- 标准(S) >
- 国际(I) >
- 自定义(C) >
- 转换为(O) >

地址: 632 (278h) 值: 69 45h 大小: 1,355 十六进制(H) UN 小 页 W 表

具体参考

<https://xz.aliyun.com/t/8062#toc-1>

修改完毕，就能得到一个有着 pdf 图标的 lnk 文件了。



但是注意到左下角还是有小箭头

关于为什么这样修改能成功的原理，我们可以做一个小实验。
这里单独新建一个文件 txt 文件



后缀改为 pdf



发现被自动关联为 pdf 图标了

010editor 查看

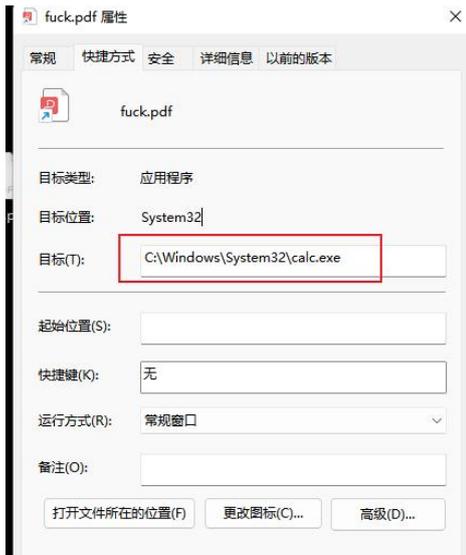


可以看到，系统并不是根据文件头来识别和关联 pdf 文件，只要后缀为 pdf 即可关联。因此通过修改后缀为./1.pdf 的方式，能够达到系统关联图标的效果，从而达到伪装的效果。

2、如何让 lnk 执行恶意代码

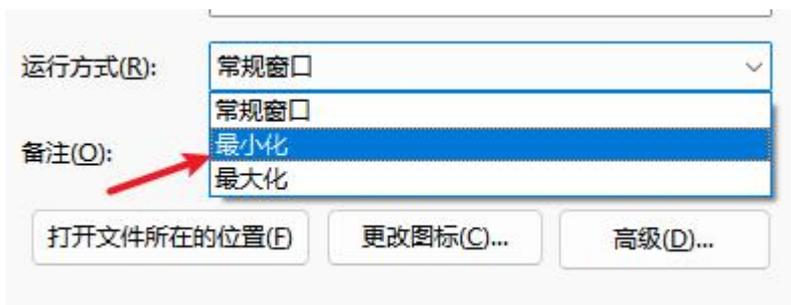
其实就和计算器一样

只要把这里的

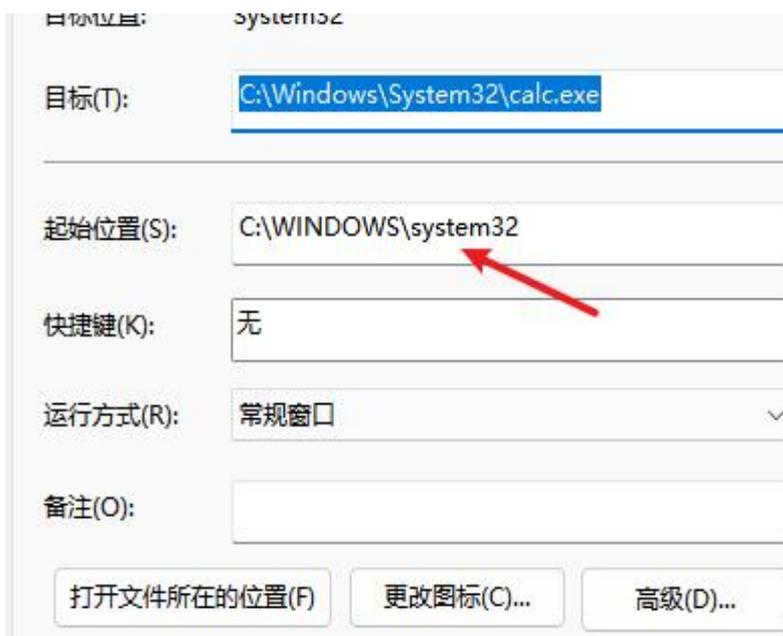


目标里的 calc.exe
换成恶意代码就行了

这里还有个小细节值得注意
这里的文件属性，需要修改为最小化，从而达到隐藏黑框的目的



并且初始生成的 Ink 文件含有初始位置 path



实战的时候记得删掉，不然这个 `lnk` 文件执行相对路径的命令的时候，总是以这个位置为起点来执行，命令并不能执行成功。