对 Redis 在 Windows 下的利用方式思考

我写的文章永远都是那么的又臭又长又菜。

前言

上次写了一篇有关 `SSRF` 打 `Redis` 主从的文章，居然被人喷了！！！说我根本就没有复现过张嘴就来？？？ 我没有理会，然后又有朋友在群问，`Redis` 在 `Windows` 环境下没有 `WEB` 如何利用？我说可以往目标尝试写 `DLL` 做劫持或者写 `LNK` 来欺骗管理员等方法，迂回的打。但 `TMD` 我又被喷了！ 非要跟我抬杠，说 `Redis` 写文件会有一些版本信息什么的一堆脏数据，根本无法写出正常 `DLL`、`EXE`、`LNK` 等文件！我说，可以参照 `Github` 上面的 `Redis` 主从 `RCE` 脚本，改改就能写出干净的文件。就因为没有现成的工具，然后就是不听？ 就是要喷！ `TMD` 的真是“天不生你键盘侠，喷道万古如长夜。”佩服佩服！不过也挺感谢这些喷子的，偶尔遇到几个喷子还能刺激我做些事情，写写博客和工具，这一番刺激又给伸手党贡献了一个脚本，当然我也希望能抛砖引玉，希望有大佬能再多发几个 `Windows` 下 `Redis` 的利用思路。

正文

首先我们知道，`Redis` 官方是没有提供 `Windows` 版的安装包的，所以目前为止基本上所有的更新和版本迭代都是 `Linux` 的，也就是说现在官方的 `Linux` 版 `Redis` 已经更新到了 `6.X` 的版本，而由微软开放技术小组所开发和维护的 `Windwos` 下使用的 `Redis` 还是 `3.X` 的版本。所以什么想在 `Windows` 下加载 `DLL` 打主从，估计还是没戏的。

目前网上公开的对 `Windows` 下的 `redis` 的利用方法：

1. 往 `WEB` 目录写马
2. 写启动项

这两项方法对写出的文件都没有严格的内容要求，即使有脏数据也不会影响最终的效果。

本文公开部分其他潜在的攻击方法：

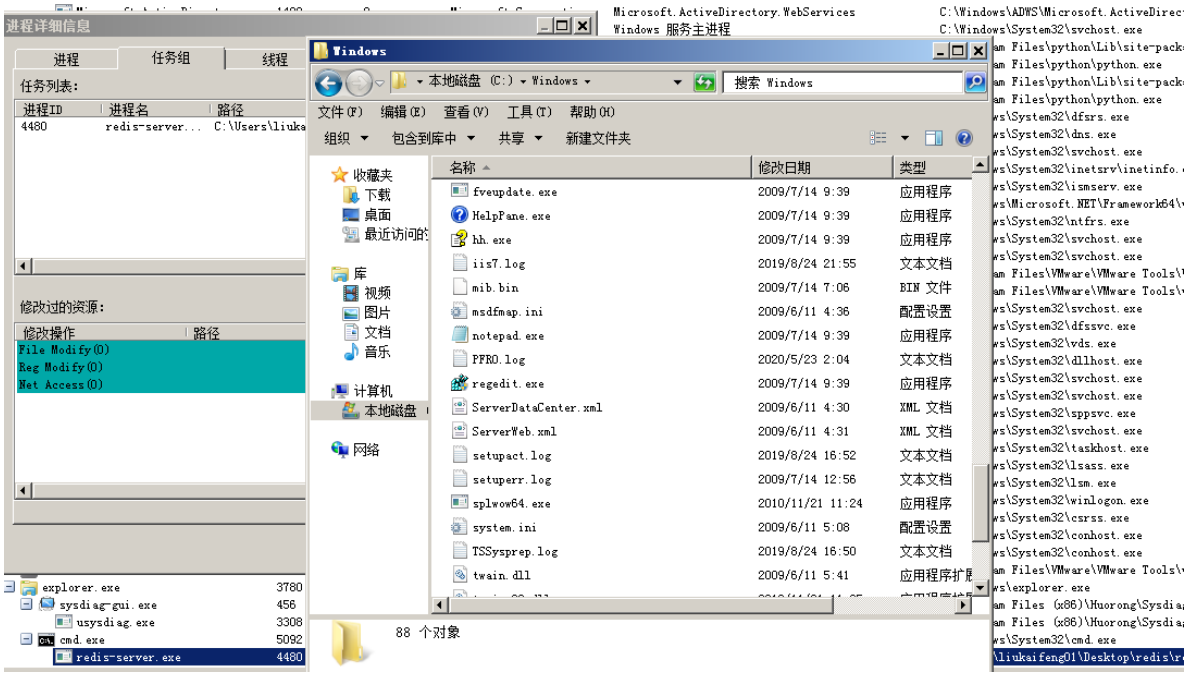
1. 系统 `DLL` 劫持 （目标重启或注销）
2. 针对特定软件的 `DLL` 劫持（目标一次点击）
3. 覆写目标的快捷方式 （目标一次点击）
4. 覆写特定软件的配置文件达到提权目的 （目标无需点击或一次点击）
5. 覆写 `sethc.exe` 等文件 （攻击方一次触发）

这些方法由于写出的是二进制或者不允许有杂质的文件所以对写出的文件有着严格的内容要求。

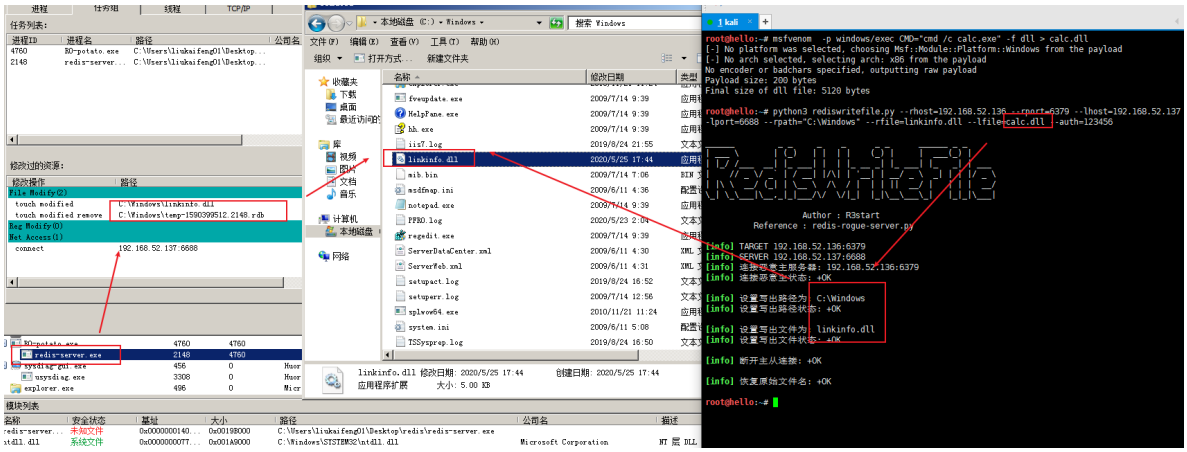
系统 `DLL` 劫持

这里以劫持 `linkinfo.dll` 为例

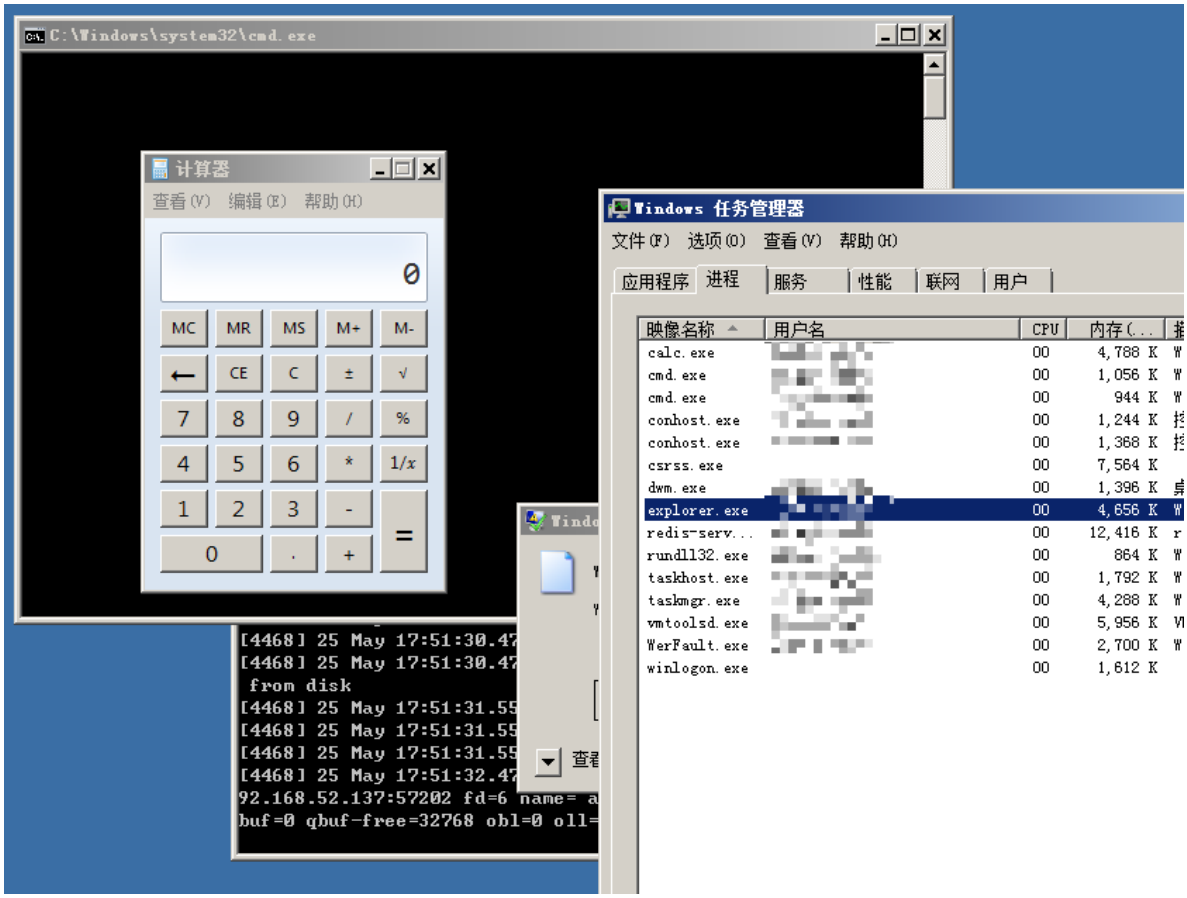
我们知道 `explorer.exe` 进程会在每次启动时自动加载 `linkinfo.dll`，所以我们可以利用它来控制目标主机，我们只需要把 `linkinfo.dll` 写入到 `C:\Windows\` 目录下即可



这里使用 `msf` 生成一个 `dll` 弹个 `calc.exe` 然后写入目标即可

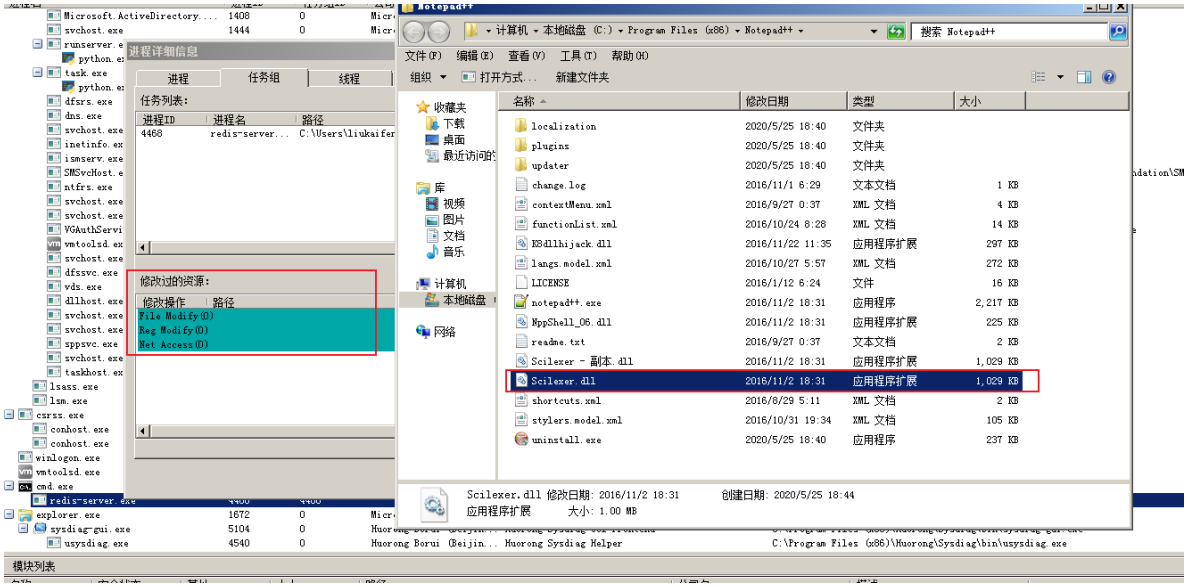


当 `explorer.exe` 被重新启动时 `DLL` 就会被执行 (应该是 `DLL` 没搞好，崩溃了，执行完以后没进入桌面，建议使用前本地调试)

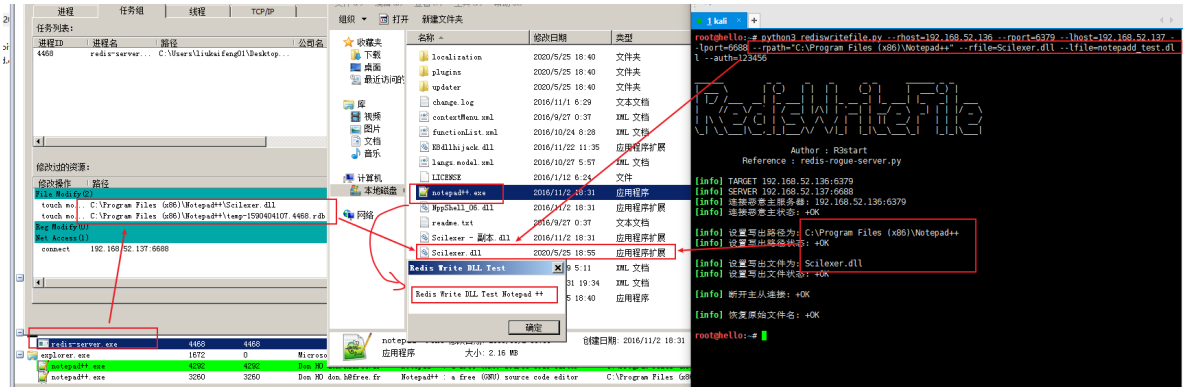


针对特定软件的 DLL 劫持

其实没什么好写的，只是提供个思路，这里以 `notepad++` 为例因为遇到的不会太多 （奸笑）



覆写 `DLL` 后当管理员打开 `Notepad++` 就会触发我们的恶意 `DLL`

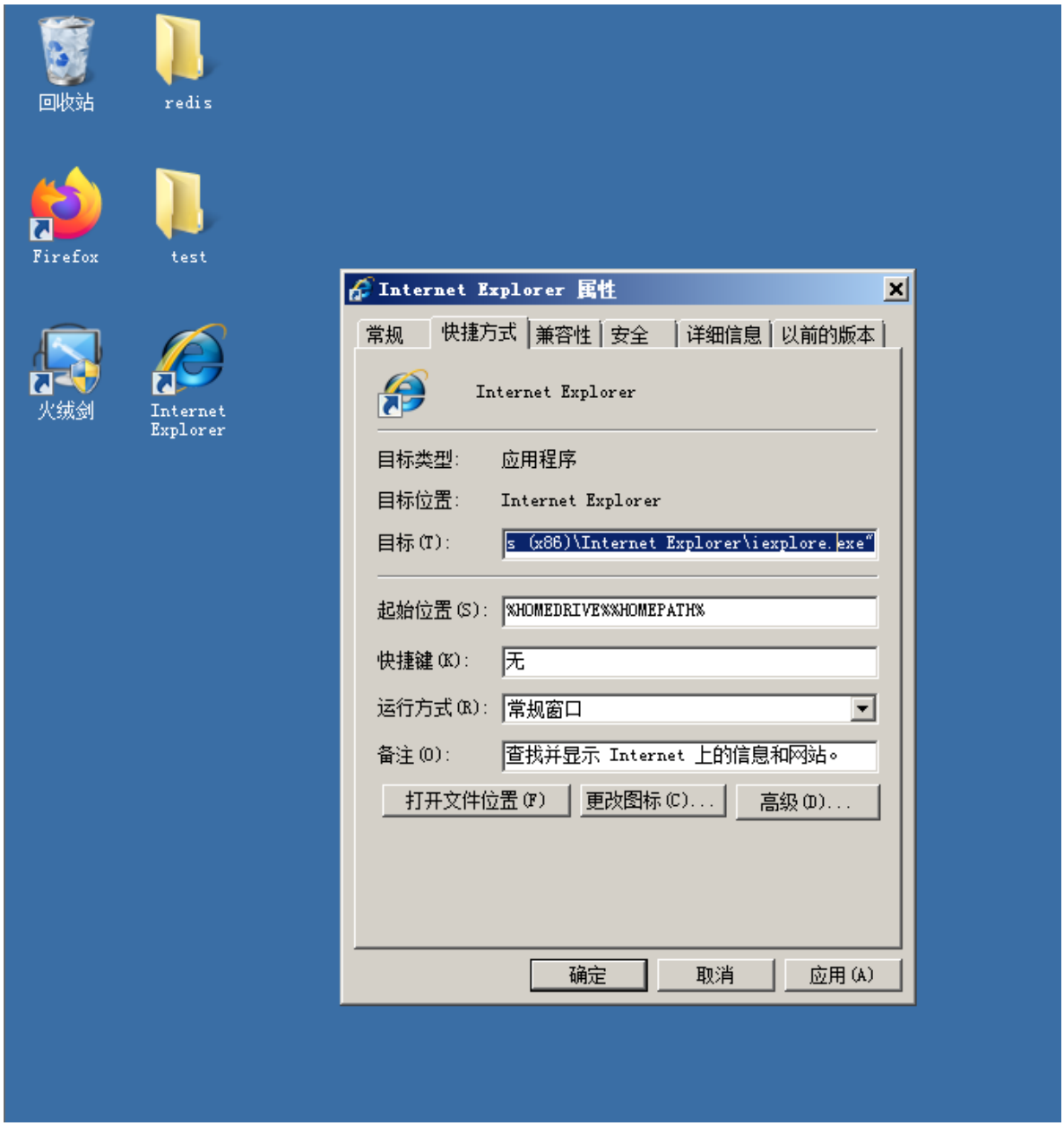


动图：

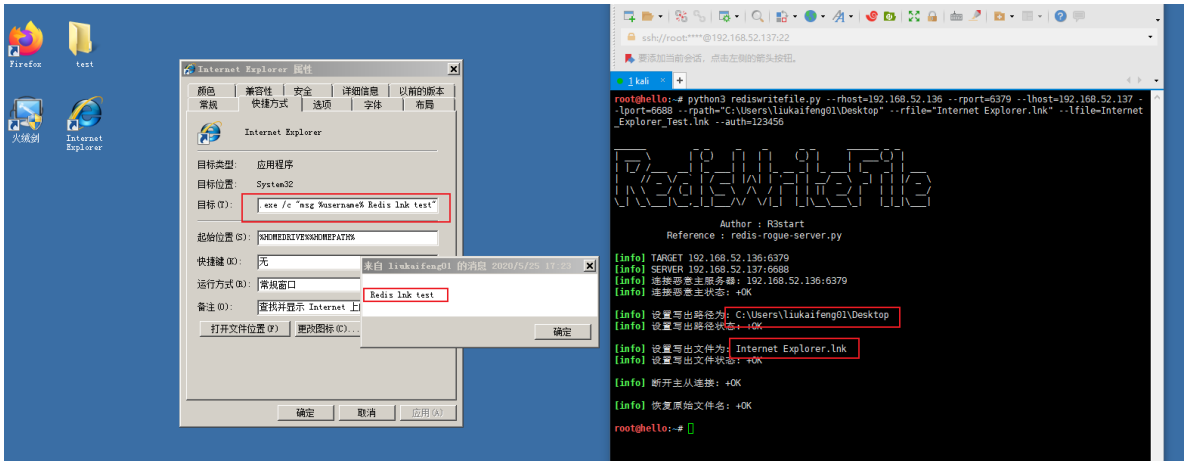
快捷方式覆写

使用 `redis` 覆写目标桌面的快捷键达到上线效果。

覆写前：



覆写后：



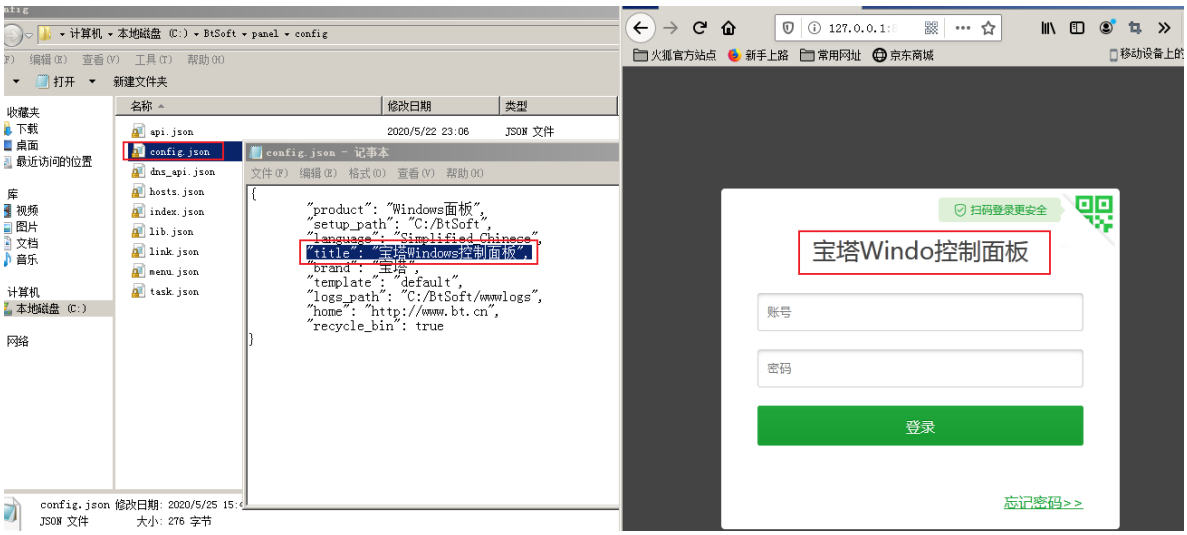
动图:

覆写特定软件的配置文件达到提权目的

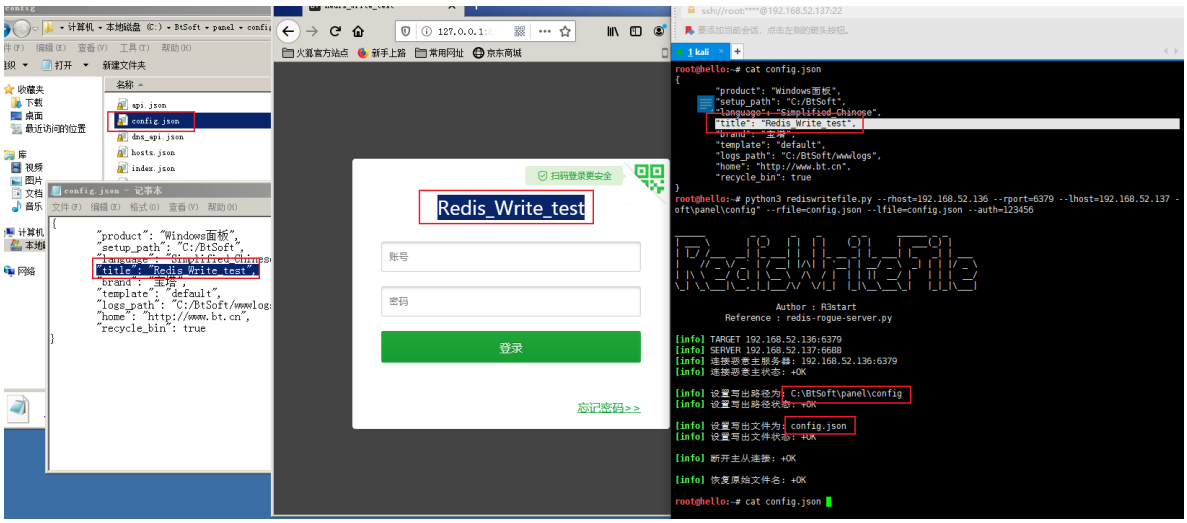
这里以宝塔为例。仅修改 `title` 让前端展示发生变化（可修改其他文件使目标上线）

宝塔的配置文件默认在 `\BtSoft\panel\config` 文件夹中，尝试使用 `Redis` 覆写 `config.json` 修改它的 `title` 配置文件是 `json` 的格式，所以覆写的时候最好不要有其他垃圾数据，此脚本刚好解决这个问题 :)

覆写前



覆写后



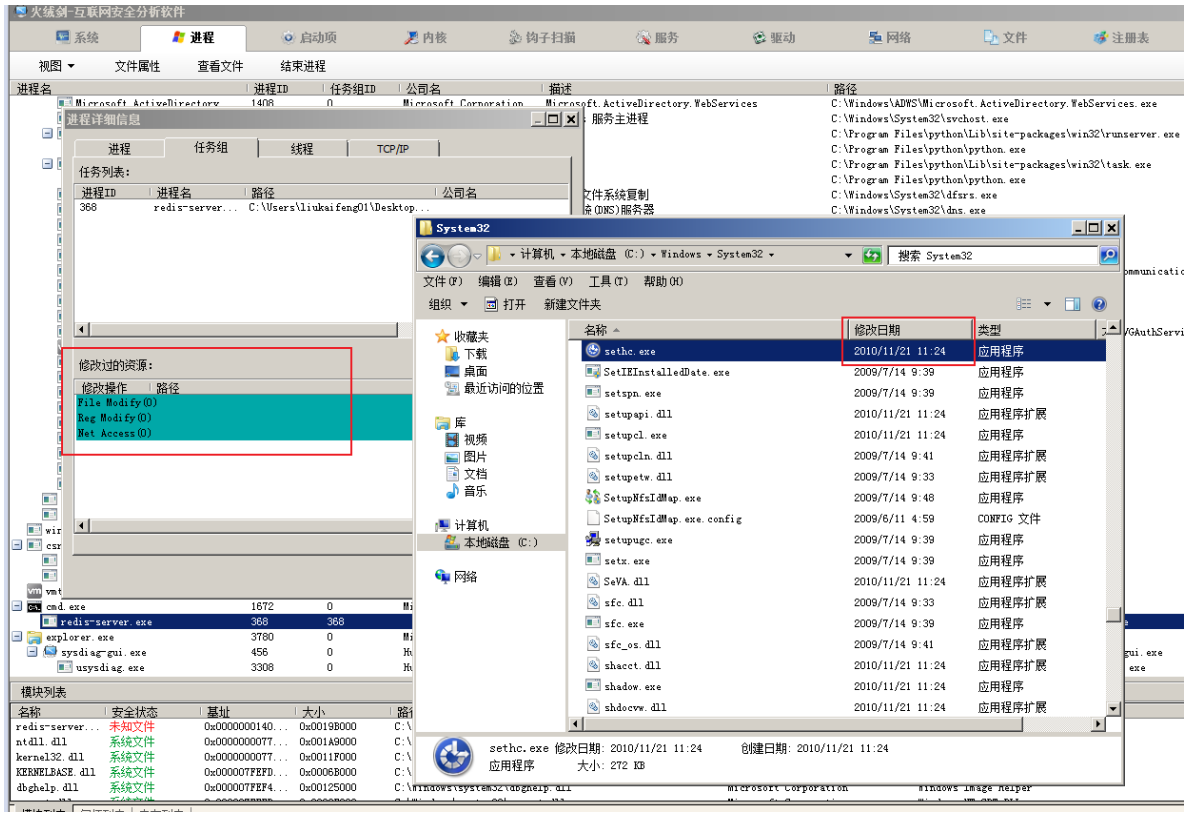
还可以覆写宝塔的其他文件使目标上线，大家可以自己摸索一下。 :D

动图：

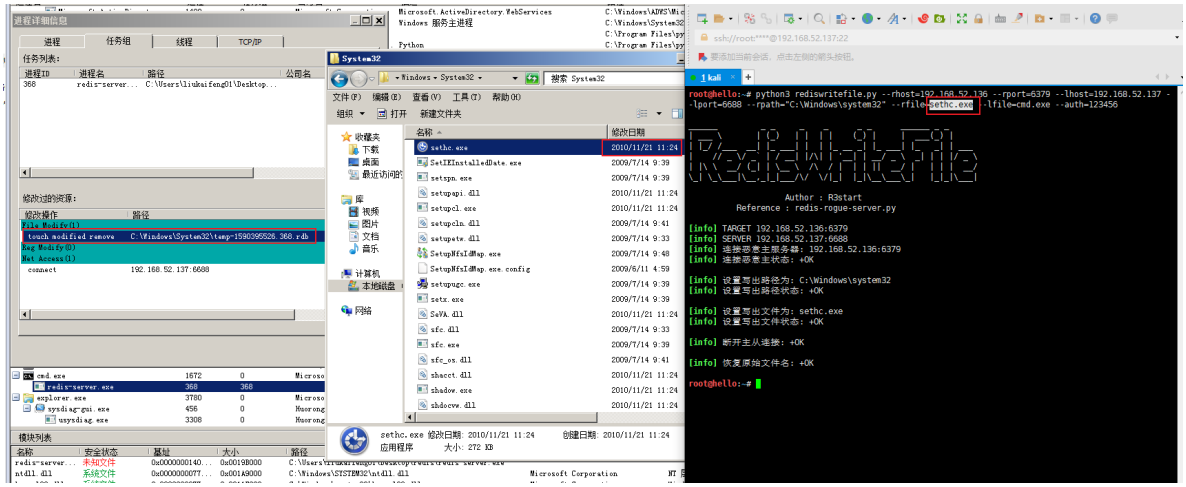
高权限下可覆写 sethc.exe 等可单向触发的文件

我这使用火绒剑监控 `redis` 的进程，然后用 `Kali` 打 `redis` 写文件，看是否有写的操作和是否写入成功。

没有打之前 `Redis` 的服务端没有并没有修改过任何资源， `sethc.exe` 的创建日期是 `2010/11/21`

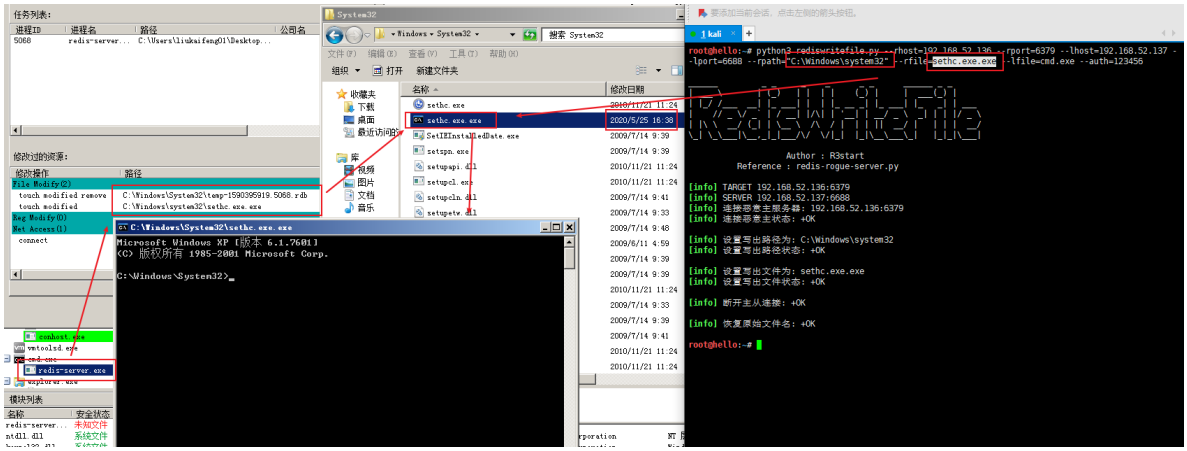


打完以后可以看到 `redis` 的服务端确实有做修改的操作，但是并没有成功而 `sethc.exe` 也并没有被修改



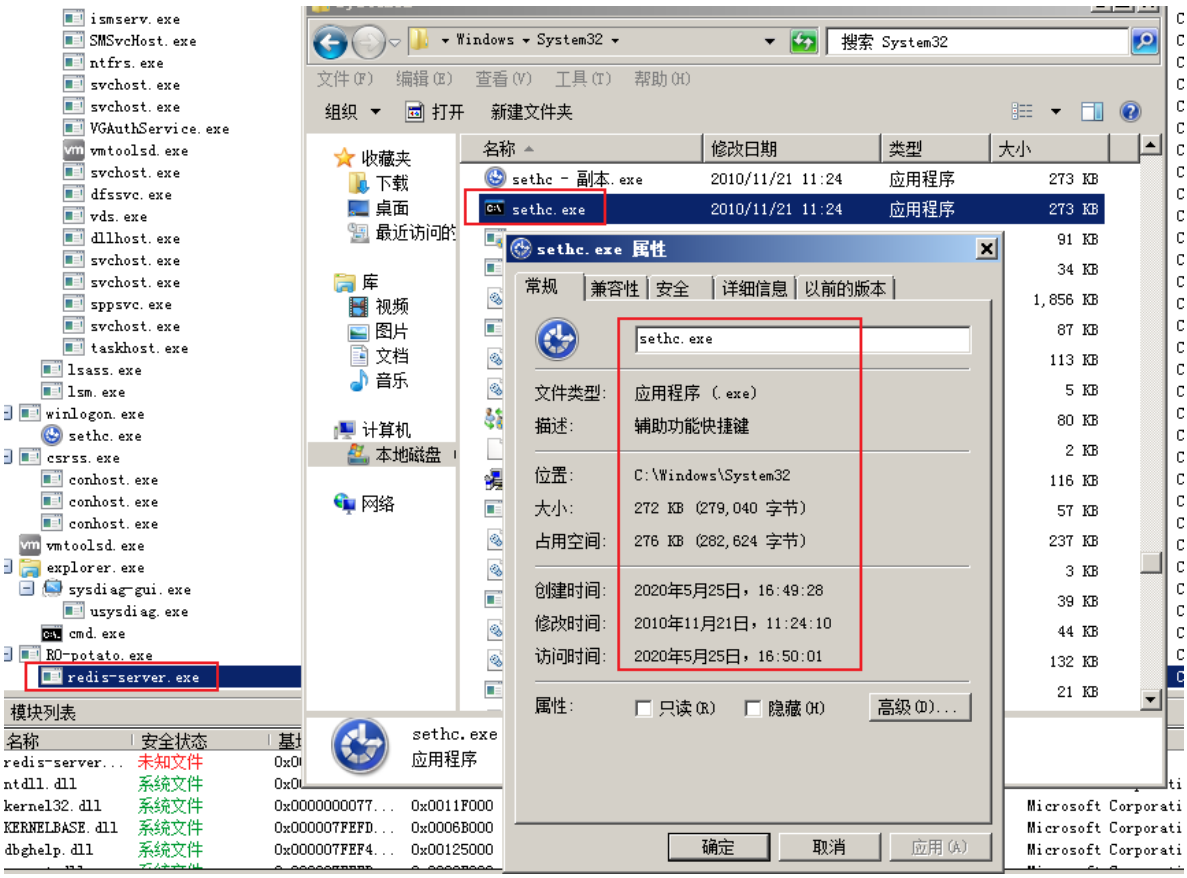
当我以为是没有权限写 `C:\windows\system32` 目录的时候，我发现并不是，我可以往这个目录下写入任意不存在的文件文件，但是却不能覆写已存在的文件，别的路径却可以，看来是有保护机制。（终究还是权限的原因）

尝试往 `C:\windows\system32` 目录下写入 `sethc.exe.exe` 测试目录是否可写，发现是可以轻易写入的

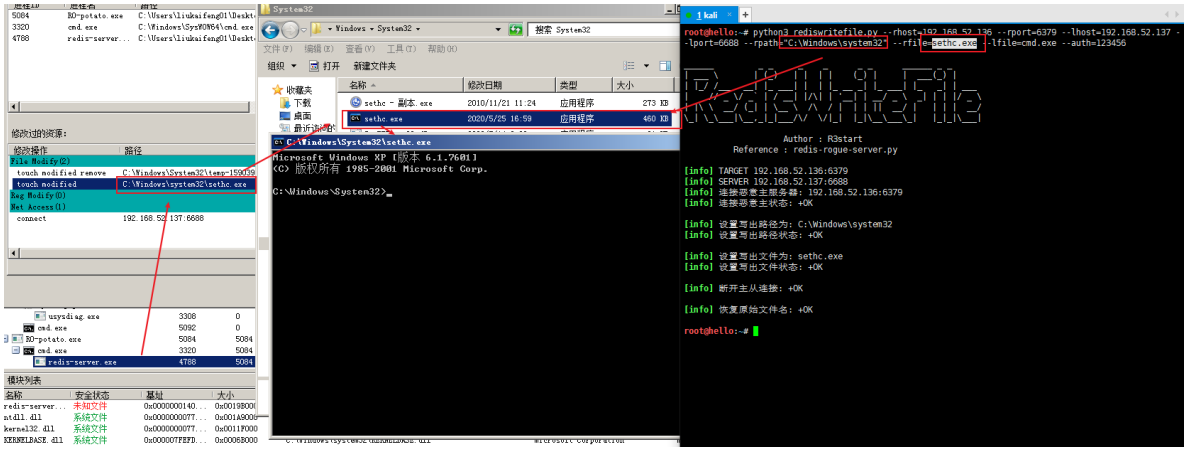


但当 `Redis` 是以 `SYSTEM` 权限启动时就可以覆写 `sethc` 实施 `sethc` 后门攻击（写文章时先打了一遍，导致 `sethc` 的图标变成了 `cmd` 图标的了... 但其实是正常的和上面的时间大小都是一致的）

打之前



打之后，可以看到只要权限足够 `redis` 也是可以通过覆写目标 `sethc.exe` 达到控制目标服务器的效果



动图：

结尾

其实文章很 `low` ，只是看大家问过好多次 `Windows` 下的 `Redis` 怎么利用，来来回回就那两个回答，而且还再一致纠结 `Redis` 写文件有脏数据的事情，所以才觉得把它脚本化并把相关思路发出来而已，希望能够抛砖引玉吧。

`GIF` 动图版本： http://r3start.net/index.php/2020/05/25/717 或 公众号： 梦里的渗透笔记

R3start

2020年5月25日21点12分