



# R3START (HTTP://R3START.NET/)

十年生死两茫茫，不思量，自难忘。

## 对 Redis 在 Windows 下的利用方式思考

发布时间: 2020年5月25日 (<http://r3start.net/index.php/2020/05/25/717>) By r3start  
(<http://r3start.net/index.php/author/r3start>) 117 次阅读

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！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）

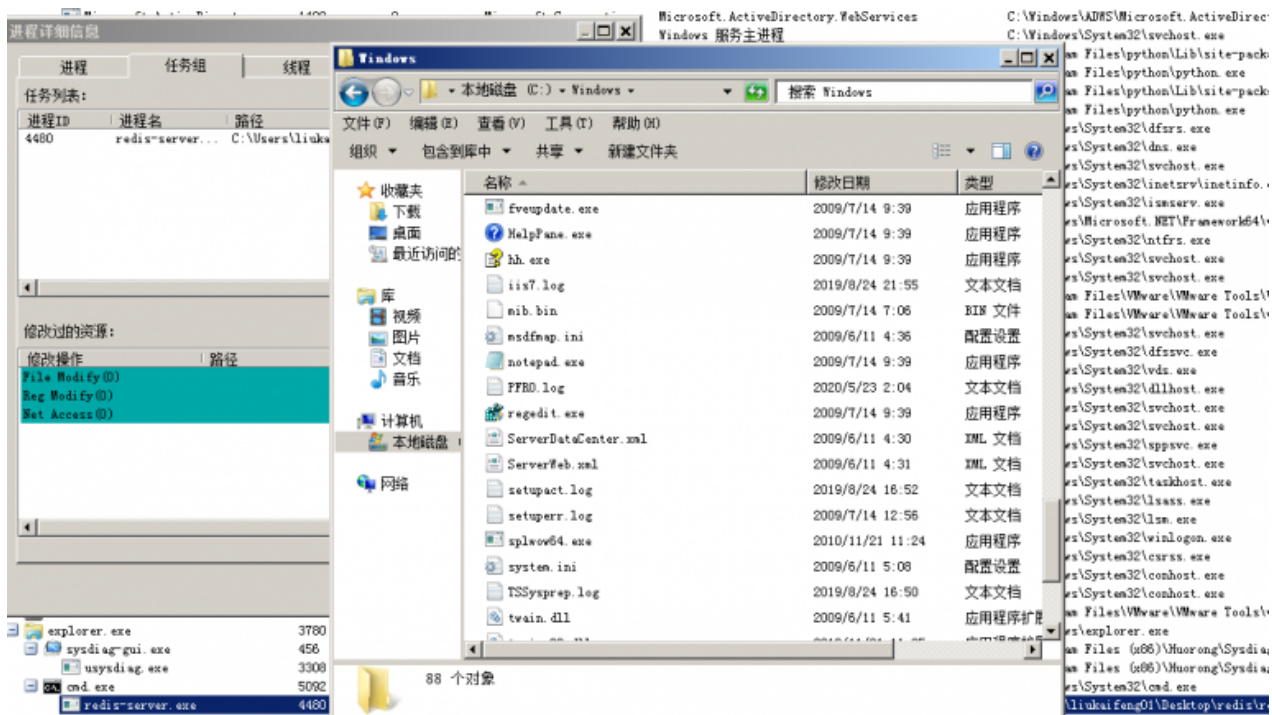
这些方法由于写出的是二进制或者不允许有杂质的文件所以对写出的文件有着严格的内容要求。

## 系统 DLL 劫持

这里以劫持 linkinfo.dll 为例

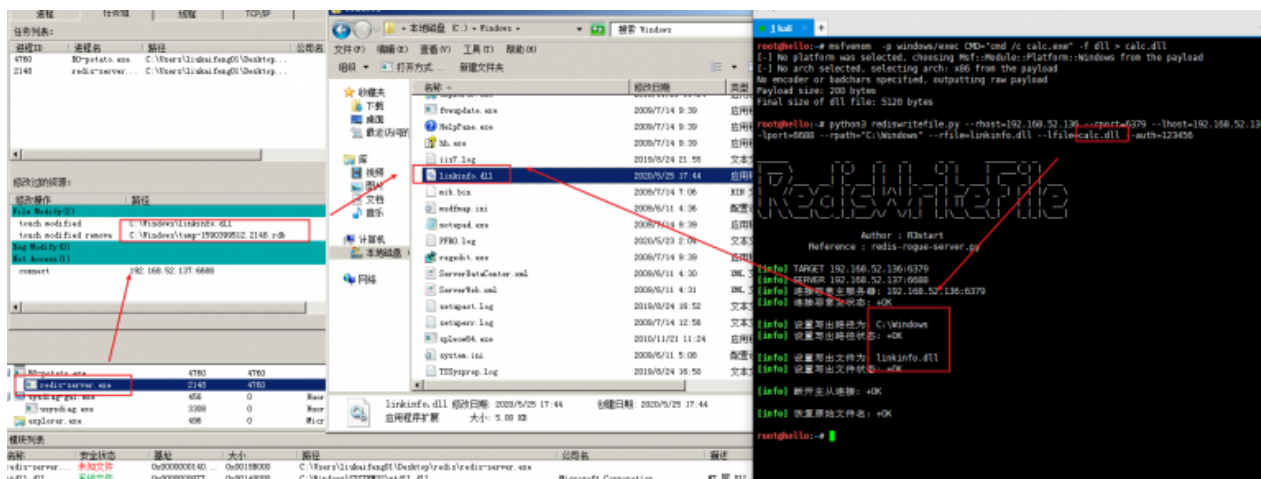
我们知道 explorer.exe 进程会在每次启动时自动加载 linkinfo.dll，所以我们可以利用它来控制目标主机，我们只需要把 linkinfo.dll 写入到 C:\Windows\ 目录下即可





(<http://r3start.net/wp-content/uploads/2020/05/2020052512390854.png>)

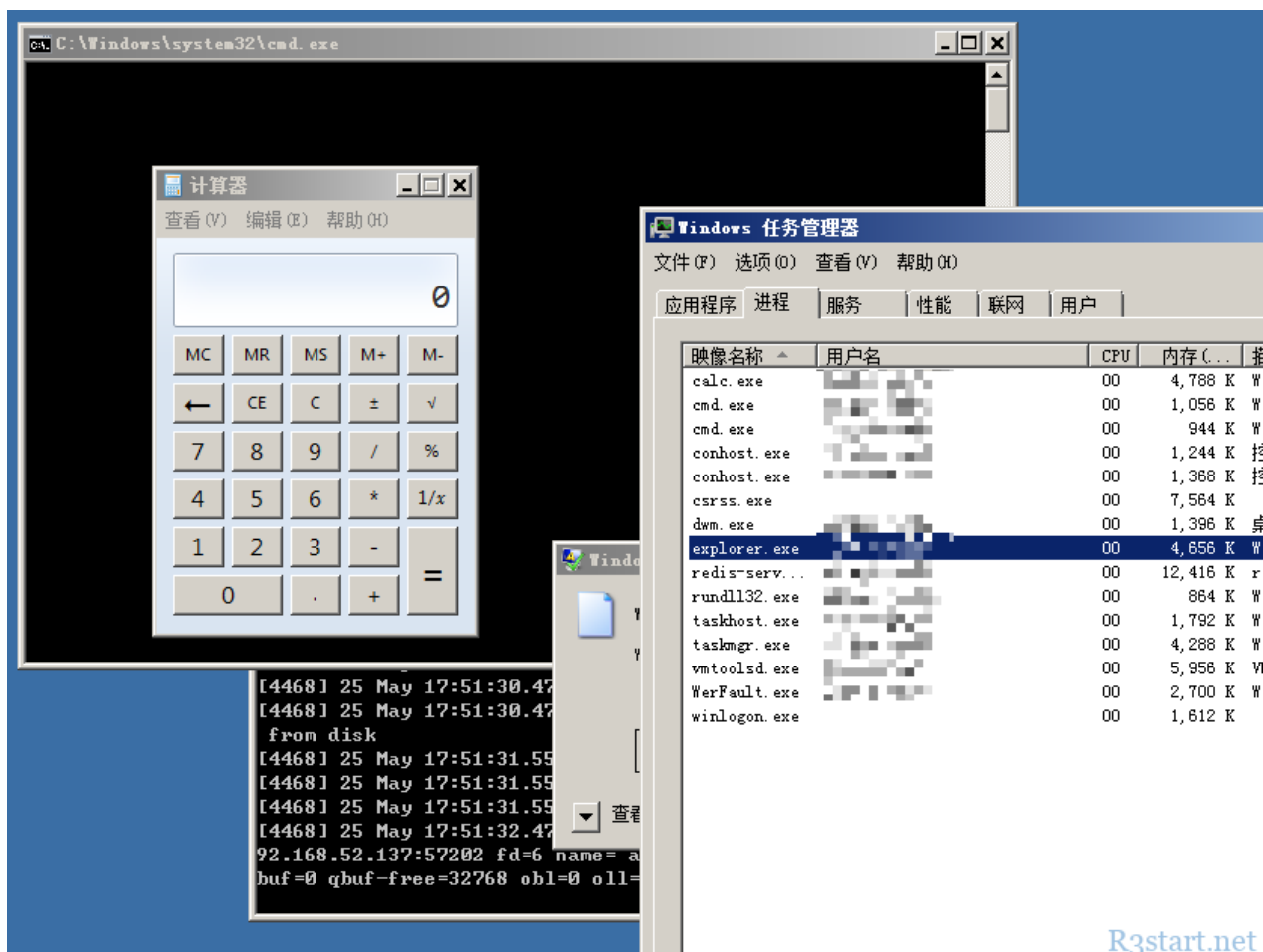
这里使用 msf 生成一个 dll 弹个 calc.exe 然后写入目标即可



(<http://r3start.net/wp-content/uploads/2020/05/2020052512395627.png>)

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)



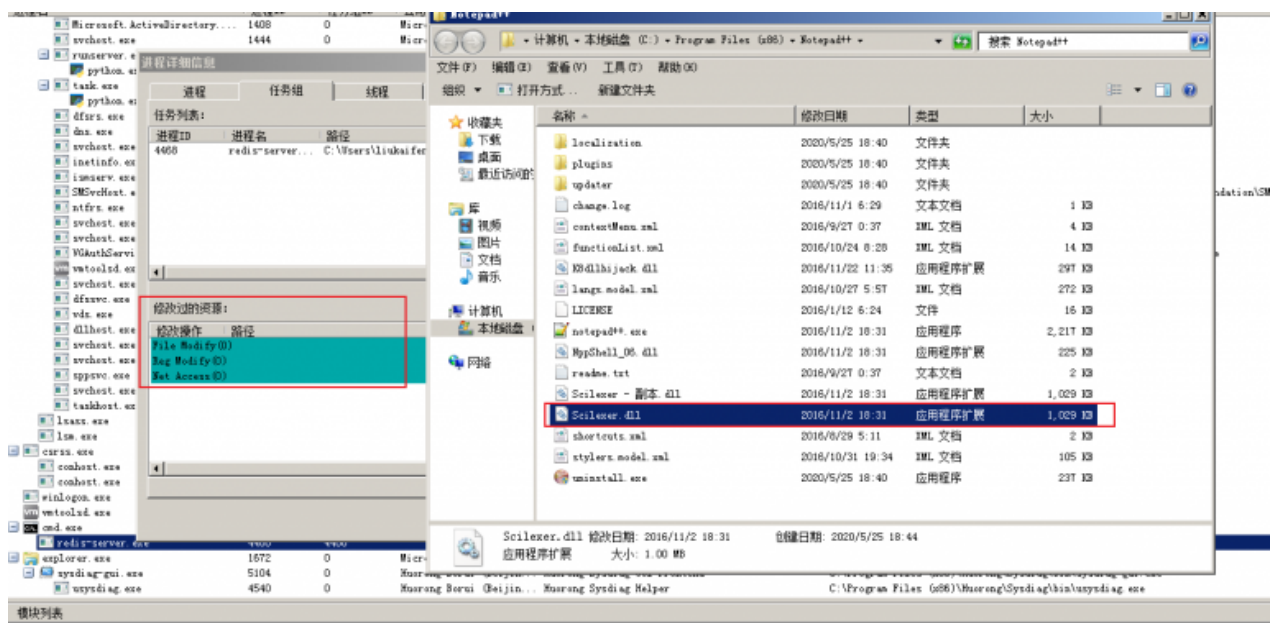


R3start.net

(<http://r3start.net/wp-content/uploads/2020/05/2020052512403157.png>)

## 针对特定软件的 DLL 劫持

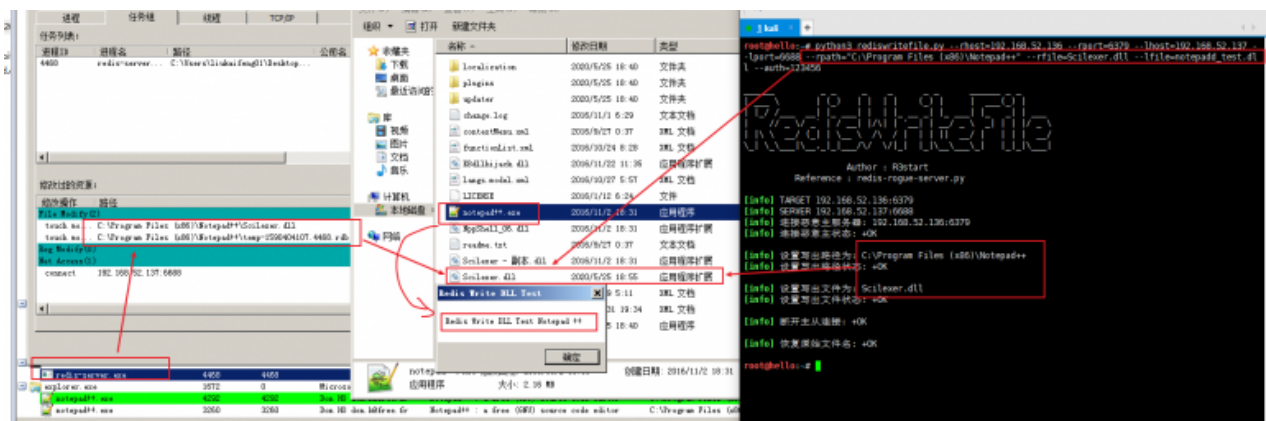
其实没什么好写的，只是提供个思路，这里以 notepad++ 为例因为遇到的不会太多（奸笑）



(<http://r3start.net/wp-content/uploads/2020/05/2020052512410678.png>)

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





(<http://r3start.net/wp-content/uploads/2020/05/2020052512413160.png>)

动图：

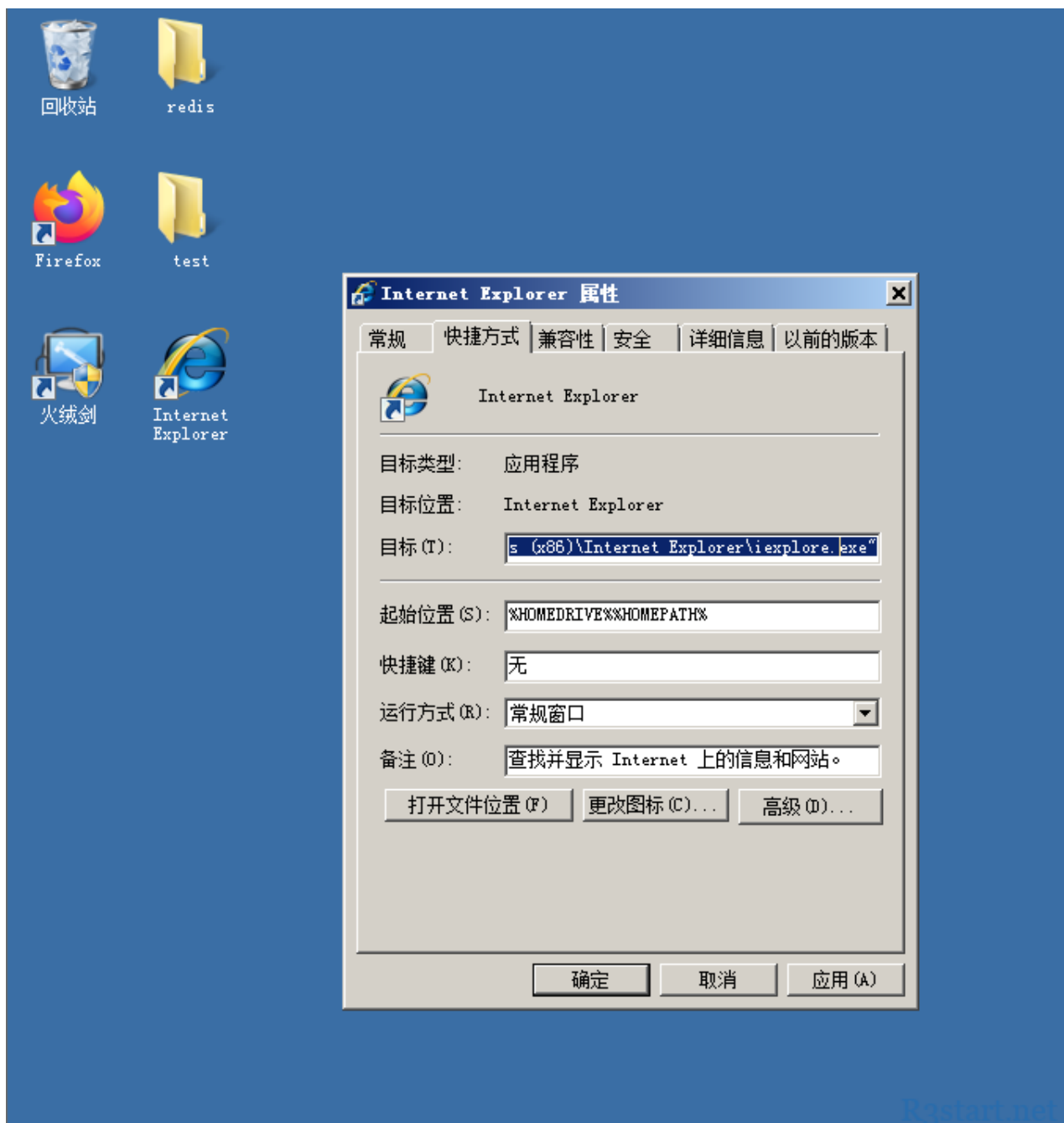


## 快捷方式覆写

使用 redis 覆写目标桌面的快捷键达到上线效果。

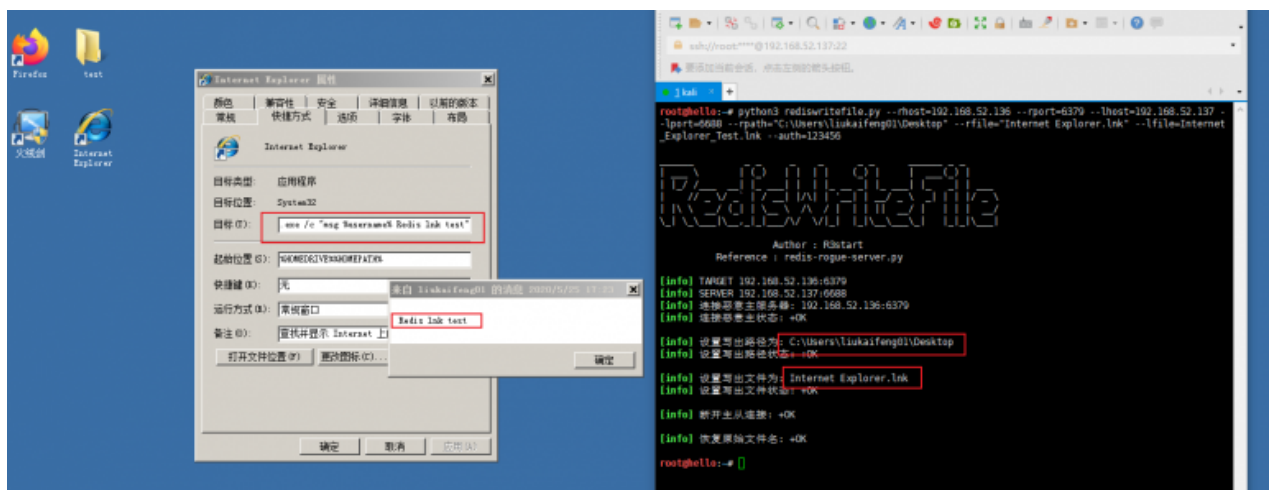
覆写前：





(<http://r3start.net/wp-content/uploads/2020/05/2020052512420443.png>)

覆写后:



(<http://r3start.net/wp-content/uploads/2020/05/2020052512423111.png>)

动图:

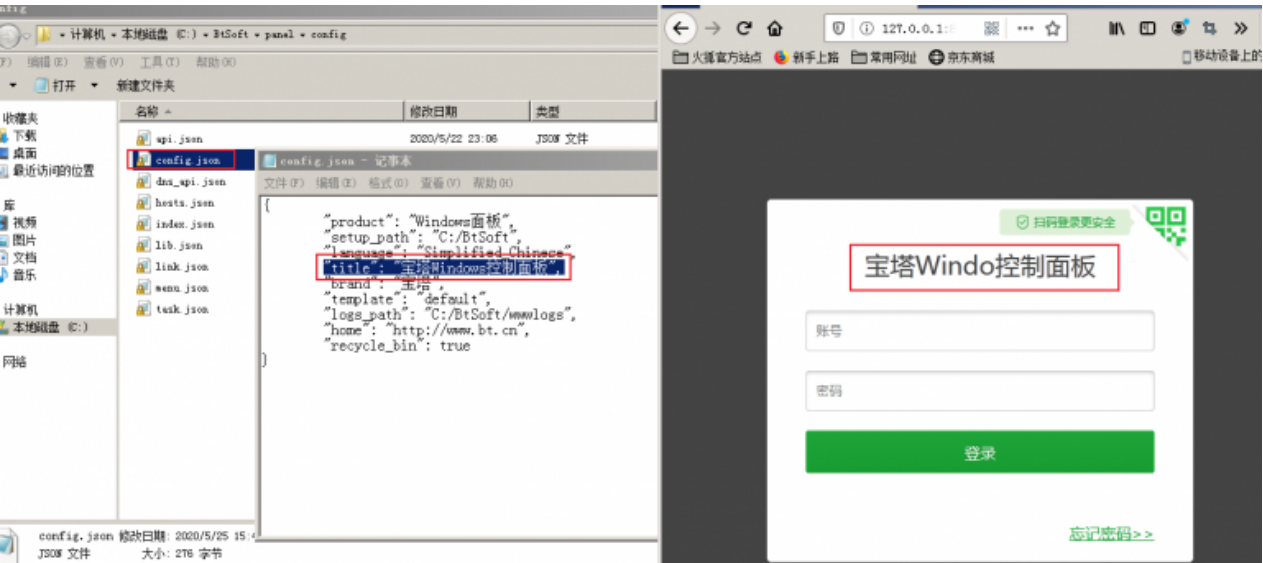


## 覆写特定软件的配置文件达到提权目的

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:

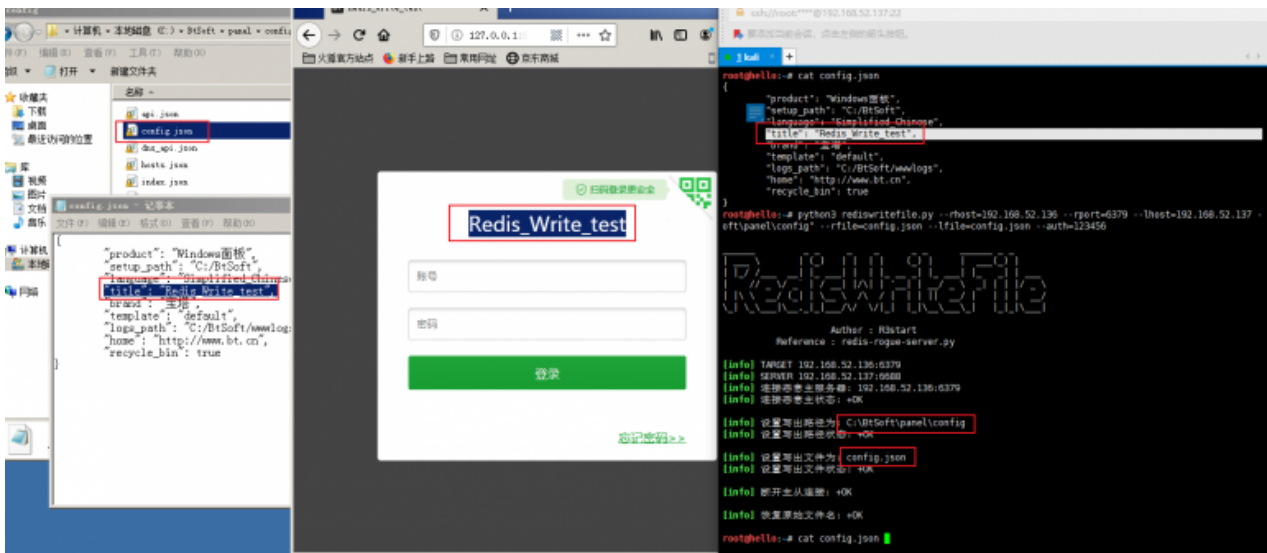


(<http://r3start.net/wp-content/uploads/2020/05/2020052512425965.png>)

覆写后:



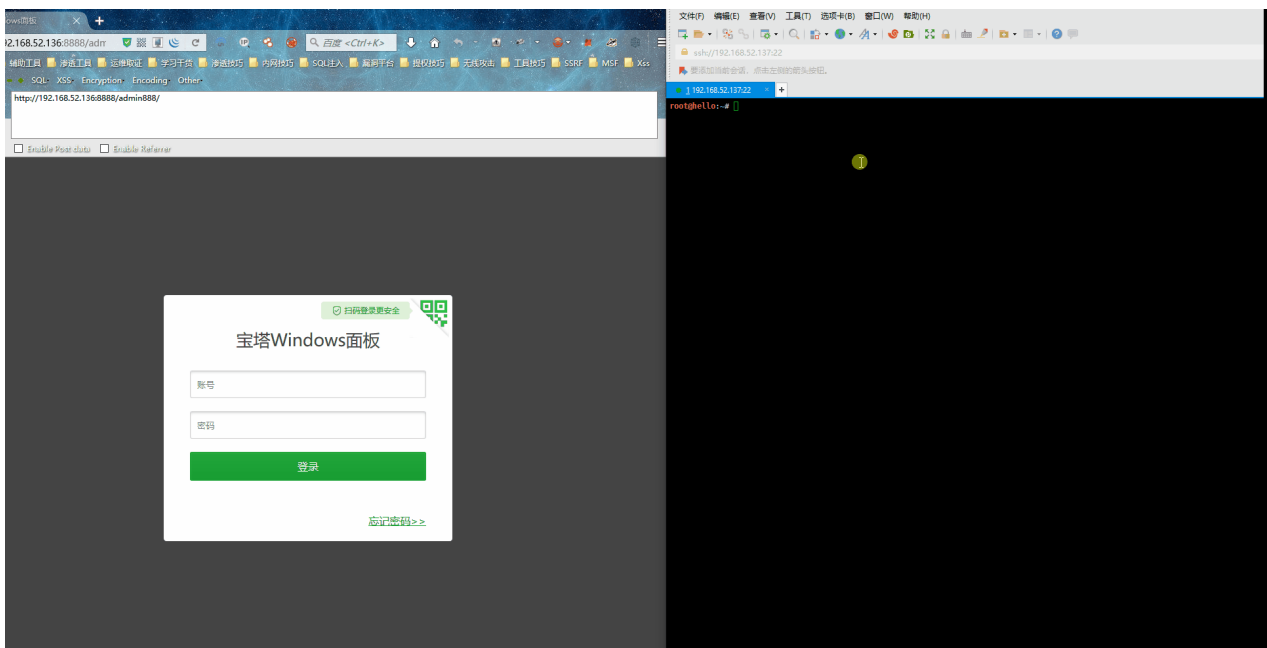




(<http://r3start.net/wp-content/uploads/2020/05/2020052512431443.png>)

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。 😊

动图:



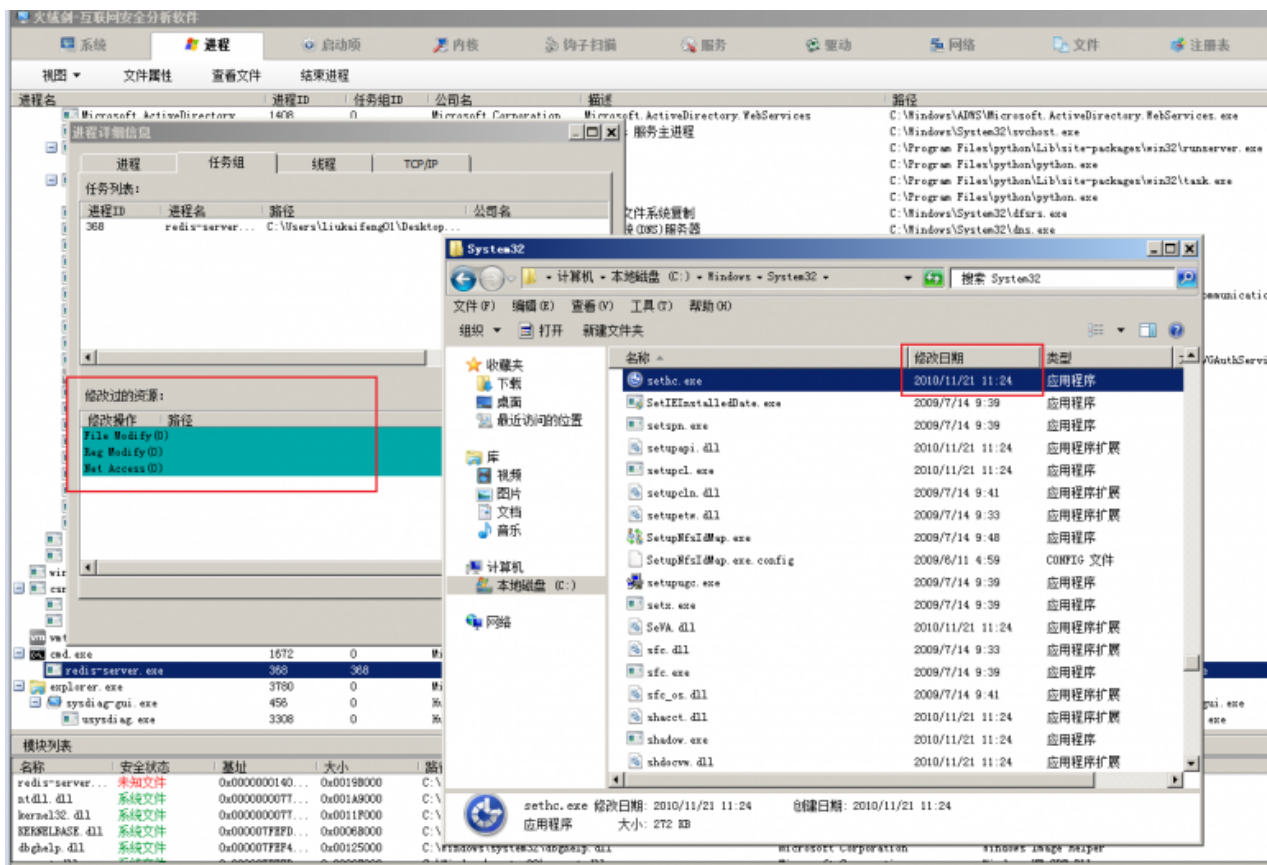
## 高权限下可覆写 sethc.exe 等可单向触发的文件

我使用火绒剑监控 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

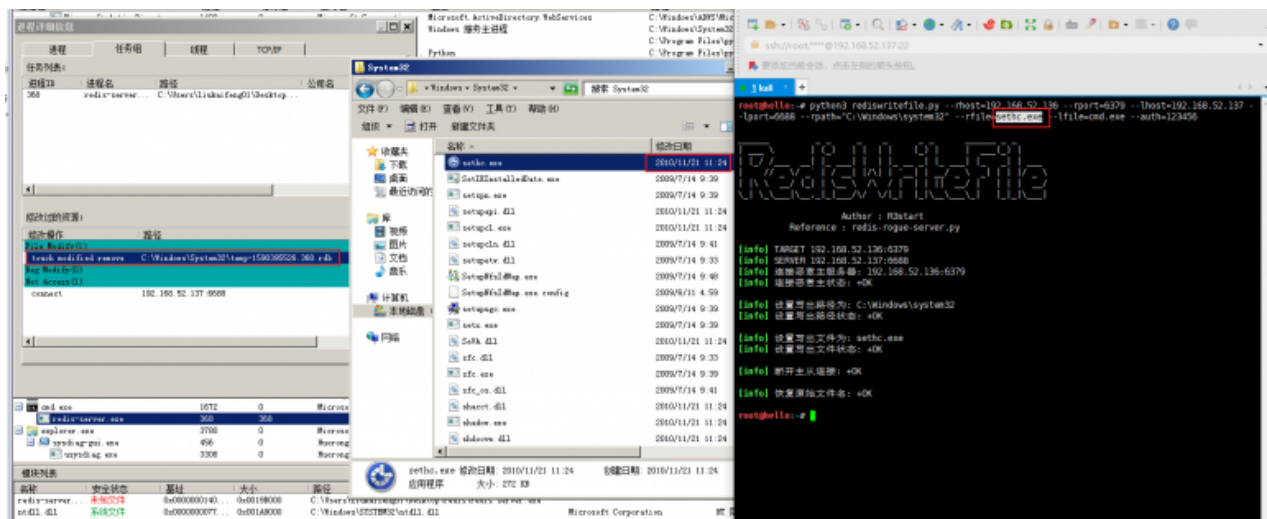






(<http://r3start.net/wp-content/uploads/2020/05/2020052512434768.png>)

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

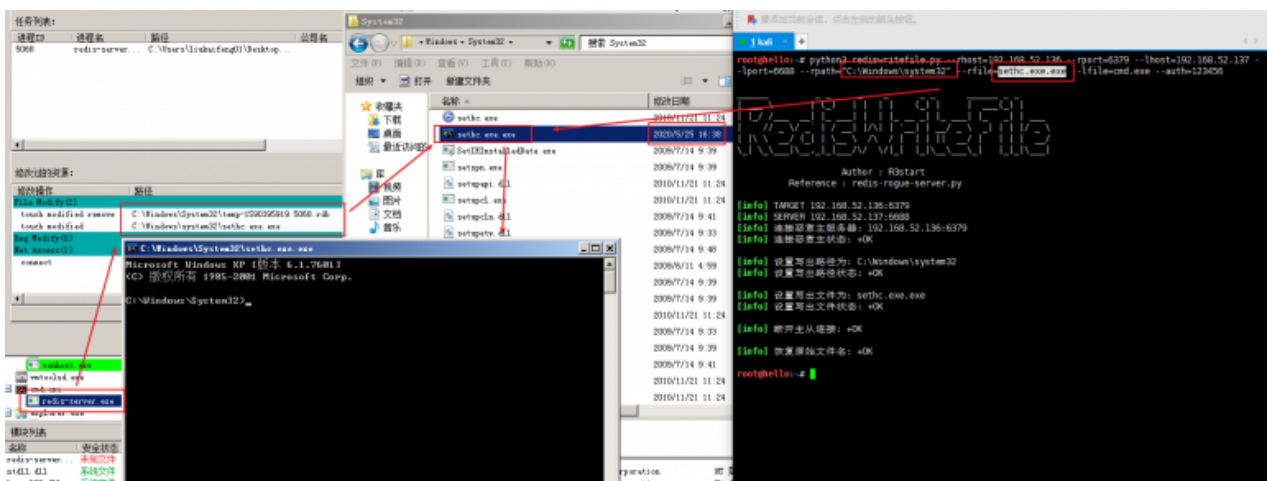


(<http://r3start.net/wp-content/uploads/2020/05/2020052512453012.png>)

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

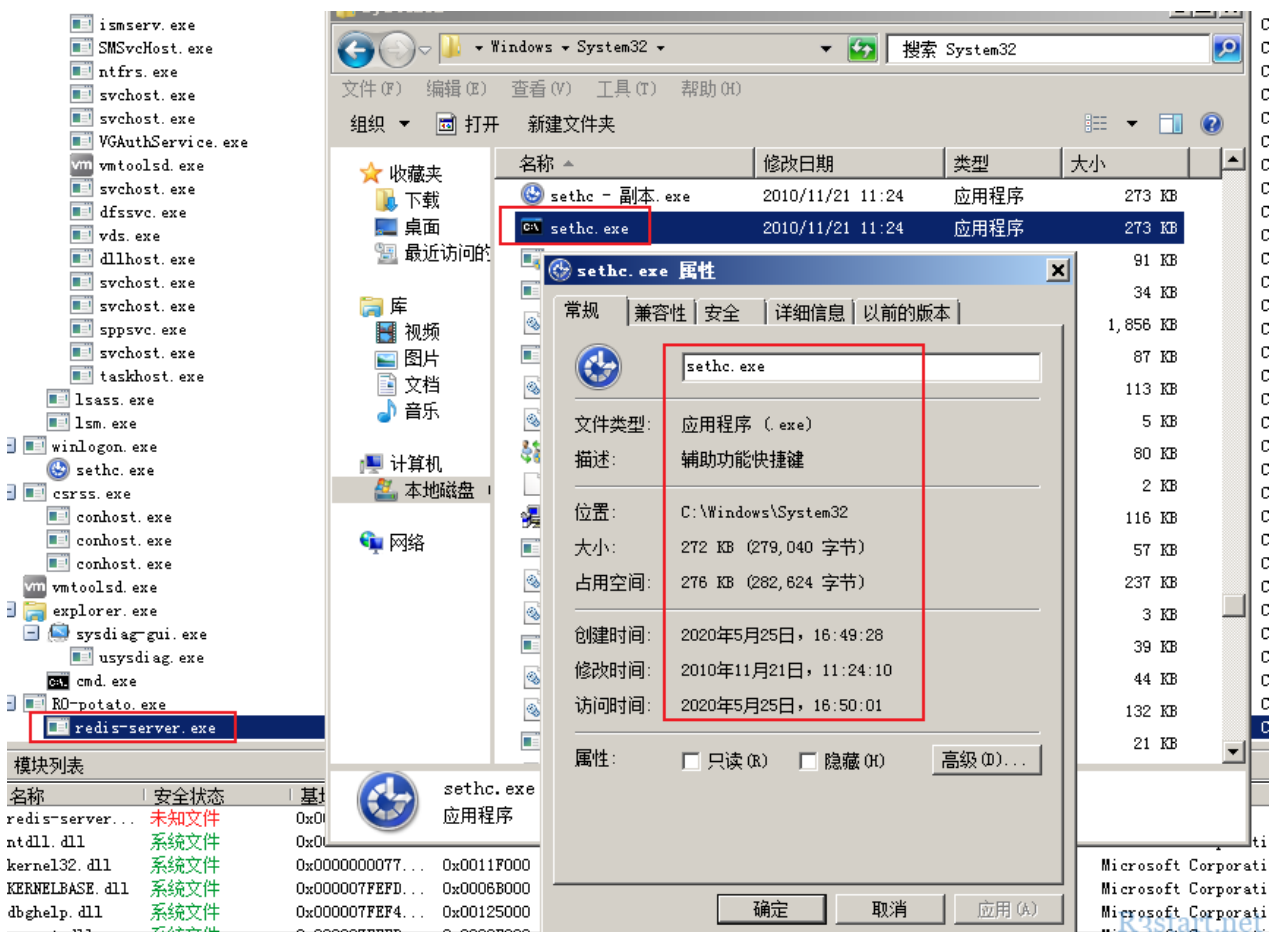




(<http://r3start.net/wp-content/uploads/2020/05/2020052512454521.png>)

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 图标了... 但其实是正常的和上面的时间大小都是一致的)

打之前



(<http://r3start.net/wp-content/uploads/2020/05/2020052512461135.png>)

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





### 3 人评论 “对 Redis 在 Windows 下的利用方式思考”

---

1.  darkless说道:

2020年5月26日 上午9:50 (<http://r3start.net/index.php/2020/05/25/717#comment-4018>)

不必理会那些喷子啊，你不给他写一个自动化利用工具，一键日卫星，他就要喷你。

回复 (<http://r3start.net/index.php/2020/05/25/717?replytocom=4018#respond>)
2.  hihi007 (<https://www.gov-cn.cn>)说道:

2020年5月26日 上午11:59 (<http://r3start.net/index.php/2020/05/25/717#comment-4021>)

时刻关注大佬的blog

回复 (<http://r3start.net/index.php/2020/05/25/717?replytocom=4021#respond>)
3.  aaaaaaaaahhhh说道:

2020年5月26日 下午8:25 (<http://r3start.net/index.php/2020/05/25/717#comment-4023>)

大佬 白嫖了一个脚本(这个无脏数据写文件真滴可以 遇到高权限的redis岂不是可以稳稳提权 之前遇到过好多高权限redis 反弹都失败估计都是因为脏数据) 可以加个球球号不

回复 (<http://r3start.net/index.php/2020/05/25/717?replytocom=4023#respond>)

### 发表评论

电子邮件地址不会被公开。 必填项已用\*标注



评论

姓名 \*

电子邮件 \*

站点

发表评论



















---

## 简介

---

ID:R3start

此博主是个没技术的屌丝。

希望能多结交几个志同道合的朋友。

Github:R35tart (<https://github.com/r35tart>)



流下了没技术的眼泪

2020年五月

—



—
4
11
18
25
( <a href="http://r3start.net/index.php/2020/05">http://r3start.net/index.php/2020/05</a>
« 3月 ( <a href="http://r3start.net/index.php/20">http://r3start.net/index.php/20</a>

---

## 文章

---

› 对 Redis 在 Windows 下的利用方式思考  
2020年5月25日

---

› 通过 SSRF 操作 Redis 主从复制写 Webshell  
2020年5月9日

---

› 陈年笔记-SQL注入一句话脱裤 2020年3月10日

---

› 记一次曲折而又有趣的渗透 2020年2月17日

---

› 有何不可? 2019年12月8日

---

## 评论

---

aaaaaaaahhhh发表在《对 Redis 在 Windows 下的利用方式思考》  
(<http://r3start.net/index.php/2020/0>





5/25/717/comment-page-1#comment-4023)》

---

hihi007 (<https://www.gov-cn.cn>)发表在《对 Redis 在 Windows 下的利用方式思考》  
(<http://r3start.net/index.php/2020/05/25/717/comment-page-1#comment-4021>)》

---

darkless发表在《对 Redis 在 Windows 下的利用方式思考》  
(<http://r3start.net/index.php/2020/05/25/717/comment-page-1#comment-4018>)》

---

hihi007 (<http://gov-cn.cn>)发表在《记一次曲折而又有趣的渗透》  
(<http://r3start.net/index.php/2020/02/17/611/comment-page-1#comment-3764>)》

---

twosmile发表在《记一次曲折而又有趣的渗透》  
(<http://r3start.net/index.php/2020/02/17/611/comment-page-1#comment-3506>)》

---

r3start发表在《记一次曲折而又有趣的渗透》  
(<http://r3start.net/index.php/2020/02/17/611/comment-page-1#comment-3488>)》

---

SSiant发表在《记一次曲折而又有趣的渗透》  
(<http://r3start.net/index.php/2020/02/17/611/comment-page-1#comment-3457>)》

---

r3的大唧唧发表在《记一次曲折而又有趣的渗透》  
(<http://r3start.net/index.php/2020/02/17/611/comment-page-1#comment-3457>)》



2/17/611/comment-page-1#comment-3315)》

---

r3start发表在《Spring Boot Actuator敏感信息泄露

(<http://r3start.net/index.php/2019/01/20/377/comment-page-1#comment-3069>)》

---

imlonghao (<https://imlonghao.com>)发表在《Spring Boot Actuator敏感信息泄露

(<http://r3start.net/index.php/2019/01/20/377/comment-page-1#comment-3067>)》

---

---

## 标签

Copyright © 2018 Powered by R3start | 粤ICP备16016122 (<http://www.miit.gov.cn/>)

51%攻击 (1)

(<http://r3start.net/index.php/tag/51gong-ji>)

Ecshop (2)

(<http://r3start.net/index.php/tag/ecshop>)

GetShell (4)

(<http://r3start.net/index.php/tag/getshell>)

Google

语法 (1) (<http://r3start.net/index.php/tag/google-yu-fa>)

GourdScan (1)

(<http://r3start.net/index.php/tag/gourdsan>)

Hacking (1)

(<http://r3start.net/index.php/tag/hacking>)

Hosts\_scan (2)

(<http://r3start.net/index.php/tag/hostsscan>)

Hydra (1)

(<http://r3start.net/index.php/tag/hydra>)

Medusa (1)

MetinfoCMS (1)

(<http://r3start.net/index.php/tag/metinfocms>)

MSF (1) (<http://r3start.net/index.php/tag/msf>)



phpmyadmin (1)  
(<http://r3start.net/index.php/tag/phpmyadmin>)  
Python (1)  
(<http://r3start.net/index.php/tag/python>) RCE  
(2)  
(<http://r3start.net/index.php/tag/rce>) SSRF (2)  
(<http://r3start.net/index.php/tag/ssrf>) ThinkPHP (3)  
(<http://r3start.net/index.php/tag/thinkphp>) VIM (1)  
(<http://r3start.net/index.php/tag/vim>) 以太坊 (1)  
(<http://r3start.net/index.php/tag/yi-tai-fang>) 以太坊私链 (1) (<http://r3start.net/index.php/tag/yi-tai-fang-si-lian>) 信息泄露 (2)  
(<http://r3start.net/index.php/tag/xin-xi-xie-lu>) 内网 (1)  
(<http://r3start.net/index.php/tag/nei-wang>) 区块链 (3)  
(<http://r3start.net/index.php/tag/qu-kuai-lian>) 区块链入门 (1)  
(<http://r3start.net/index.php/tag/qu-kuai-lian-ru-men>) 双花交易 (1)  
(<http://r3start.net/index.php/tag/shuang-hua-jiao-yi>) 命令执行 (2)  
(<http://r3start.net/index.php/tag/ming-ling-zhi-xing>) 咸鱼 (1)  
(<http://r3start.net/index.php/tag/xianyu>) 垃圾 (1)  
(<http://r3start.net/index.php/tag/laji>) 备案 (1)  
(<http://r3start.net/index.php/tag/bei-an>) 废物 (1)  
(<http://r3start.net/index.php/tag/feiwu>) 扫描 (1)  
(<http://r3start.net/index.php/tag/sao-miao>) 攻击复现 (1) (<http://r3start.net/index.php/tag/gong-ji-fu-xian>) 教程 (1) (<http://r3start.net/index.php/tag/jiao-cheng>) 注入 (2)  
(<http://r3start.net/index.php/tag/zhuru>) 渗透 (2)  
(<http://r3start.net/index.php/tag/>)



shentou) 渗透测试 (5)

([http://r3start.net/index.php/tag/shen-](http://r3start.net/index.php/tag/shen-tou-ce-shi)

[tou-ce-shi](http://r3start.net/index.php/tag/shen-tou-ce-shi)) 漏洞利用 (3)

(<http://r3start.net/index.php/tag/lou-dong-li-yong>) 爆破

(1) (<http://r3start.net/index.php/tag/bao-po>) 生活 (2)

(<http://r3start.net/index.php/tag/shenhuo>) 盲注 (1)

(<http://r3start.net/index.php/tag/mang-zhu>) 私链

(1) (<http://r3start.net/index.php/tag/si-lian>) 算力攻

击 (1) (<http://r3start.net/index.php/tag/suan-li-gong-ji>) 编程 (1)

(<http://r3start.net/index.php/tag/biancheng>) 网络

安全法 (1) (<http://r3start.net/index.php/tag/wang-luo-an-quan-fa>) 轮子 (1)

(<http://r3start.net/index.php/tag/lunzi>) 远程命令执

行 (1) (<http://r3start.net/index.php/tag/yuan-cheng-ming-ling-zhi-xing>)

---

## 友情链接

---

Snowming

(<http://blog.leanote.com/snowming>)

0x584A

(<https://www.jgeek.cn/>)

Darkeyer

(<http://darkeyer.github.io>)

Lcy (<https://phpinfo.me/>)

离别歌

(<https://www.leavesongs.com/>)

lsh4ck

(<https://www.lshack.cn/>)

R4v3zn

(<https://www.r4v3zn.com/>)



Magic\_zero

(<https://www.cnblogs.com/magic-zero/>)

黑客街

(<https://www.hackjie.com/>)

Patrilic (<https://patrilic.top/>)

伍默 (<http://wuhash.com/>)

DVP去中心化漏洞平台

(<https://dvpnet.io/>)

